debug ipv6 pim df-election

To display debug messages for Protocol Independent Multicast (PIM) bidirectional designated forwarder (DF) election message processing, use the **debug ipv6 pim df-election** command in privileged EXEC mode. To disable debug messages for PIM bidirectional DF election message processing, use the **no** form of this command.

debug ipv6 pim df-election [**interface** *type number*] [**rp** *rp-name* | *rp-address*]

no debug ipv6 pim df-election [**interface** *type number*] [**rp** *rp-name* | *rp-address*]

Syntax Description

interface	(Optional) Specifies that debug messages on a specified interface will be displayed.
type number	(Optional) Interface type and number. For more information, use the question mark (?) online help function.
rp	(Optional) Specifies that debug messages on a specified Route Processor (RP) will be displayed.
rp-name	(Optional) The name of the specified RP.
rp-address	(Optional) The IPv6 address of the specified RP.

Command Default

Debugging for PIM bidirectional DF election message processing is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **debug ipv6 pim df-election** command if traffic is not flowing properly when operating in PIM bidirectional mode or if the **show ipv6 pim df** and **show ipv6 pim df winner** commands do not display the expected information.

Examples

The following example shows how to enable debugging for PIM bidirectional DF election message processing on Ethernet interface 1/0 and at 200::1:

```
Route# debug ipv6 pim df-election interface ethernet 1/0 rp 200::1
```

Related Commands

Command	Description
ipv6 pim rp-address	Configures the address of a PIM RP for a particular group range.
show ipv6 pim df	Displays the DF-election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

debug ipv6 pim limit

To enable debugging for Protocol Independent Multicast (PIM) interface limits, use the **debug ipv6 pim limit** command in privileged EXEC mode. To restore the default value, use the **no** form of this command.

debug ipv6 pim limit [*group*]

no debug ipv6 pim limit

Syntax Description

group	(Optional) Specific group to be debugged.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Usage Guidelines

Use the **debug ipv6 pim limit** command to display debugging information for interface limits and costs. Use the optional *group* argument to specify a particular group to debug.

Examples

The following example enables PIM interface limit debugging:

```
Router# debug ipv6 pim limit
```

Related Commands

Command	Description
ipv6 multicast limit	Configures per-interface mroute state limiters in IPv6.
ipv6 multicast limit cost	Applies a cost to mroutes that match per interface mroute state limiters in IPv6.

debug ipv6 policy

To display IPv6 policy routing packet activity, use the **debug ipv6 policy** command in user EXEC or privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 policy [*access-list-name*]

no debug ipv6 policy [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default

IPv6 policy routing packet activity is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SXI4	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI4.
Cisco IOS XE Release 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

If no access list is specified using the optional *access-list-name* argument, information about all policy-matched and policy-routed packets is displayed.

After you configure IPv6 policy routing, use the **debug ipv6 policy** command to verify that IPv6 policy-based routing (PBR) is policy-routing packets normally. Policy routing looks at various parts of the packet and then routes the packet based on certain user-defined attributes in the packet. The **debug ipv6 policy** command helps you determine what policy routing is following. It displays information about whether a packet matches the criteria, and if so, the resulting routing information for the packet.

Do not use the **debug ipv6 policy** command unless you suspect a problem with IPv6 PBR policy routing.

Examples

The following example enables IPv6 policy routing packet activity. The output for this command is self-explanatory:

```
Router# debug ipv6 policy

00:02:38:IPv6 PBR:Ethernet0/0, matched src 2003::90 dst 2001:1000::1 protocol 58
00:02:38:IPv6 PBR:set nexthop 2003:1::95, interface Ethernet1/0
00:02:38:IPv6 PBR:policy route via Ethernet1/0/2003:1::95
```

debug ipv6 pool

To enable debugging on IPv6 prefix pools, use the debug ipv6 pool command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ipv6 pool

no debug ipv6 pool

Syntax Description

This command has no keywords or arguments.

Command Default

No debugging is active.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.

Examples

The following example enables debugging for IPv6 prefix pools:

```
Router# debug ipv6 pool

2w4d: IPv6 Pool: Deleting route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
2w4d: IPv6 Pool: Returning cached entry 2001:0DB8::/29 for cisco on Virtual-Access1 to
pool1
2w4d: IPv6 Pool: Installed route/prefix 2001:0DB8::/29 to Virtual-Access1 for cisco
```

Related Commands

Command	Description
ipv6 local pool	Configures a local IPv6 prefix pool.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
show ipv6 local pool	Displays information about defined IPv6 prefix pools.

debug ipv6 rip

To display debug messages for IPv6 Routing Information Protocol (RIP) routing transactions, use the **debug ipv6 rip** command in privileged EXEC mode. To disable debug messages for IPv6 RIP routing transactions, use the **no** form of this command.

debug ipv6 rip [*interface-type interface-number*]

no debug ipv6 rip [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) The interface type about which to display debug messages.
interface-number	(Optional) The interface number about which to display debug messages.

Command Default

IPv6 RIP debugging is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **debug ipv6 rip** command is similar to the **debug ip rip** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Using this command without arguments enables IPv6 RIP debugging for RIP packets that are sent and received on all router interfaces. Using this command with arguments enables IPv6 RIP debugging for RIP packets that are sent and received only on the specified interface.

Caution Using this command on busy networks seriously degrades the performance of the router.

Examples

The following example shows output for the **debug ipv6 rip** command:

```
Router# debug ipv6 rip

13:09:10:RIPng:Sending multicast update on Ethernet1/1 for as1_rip
13:09:10:        src=FE80::203:E4FF:FE12:CC1D
13:09:10:        dst=FF02::9 (Ethernet1/1)
13:09:10:        sport=521, dport=521, length=32
13:09:10:        command=2, version=1, mbz=0, #rte=1
13:09:10:        tag=0, metric=1, prefix=::/0
13:09:28:RIPng:response received from FE80::202:FDFF:FE77:1E42 on Ethernet1/1 for as1_rip
13:09:28:        src=FE80::202:FDFF:FE77:1E42 (Ethernet1/1)
13:09:28:        dst=FF02::9
13:09:28:        sport=521, dport=521, length=32
13:09:28:        command=2, version=1, mbz=0, #rte=1
13:09:28:        tag=0, metric=1, prefix=2000:0:0:1:1::/80
```

The example shows two RIP packets; both are updates, known as “responses” in RIP terminology and indicated by a “command” value of 2. The first is an update sent by this router, and the second is an update received by this router. Multicast update packets are sent to all neighboring IPv6 RIP routers (all routers that are on the same links as the router sending the update, and that have IPv6 RIP enabled). An IPv6 RIP router advertises the contents of its routing table to its neighbors by periodically sending update packets over those interfaces on which IPv6 RIP is configured. An IPv6 router may also send “triggered” updates immediately following a routing table change. In this case the updates only includes the changes to the routing table. An IPv6 RIP router may solicit the contents of the routing table of a neighboring router by sending a Request (command =1) message to the router. The router will respond by sending an update (Response, command=2) containing its routing table. In the example, the received response packet could be a periodic update from the address FE80::202:FDFF:FE77:1E42 or a response to a RIP request message that was previously sent by the local router.

Table 24 describes the significant fields shown in the display.

Table 24 debug ipv6 rip Field Descriptions

Field	Description
as1_rip	The name of the RIP process that is sending or receiving the update.
src	The address from which the update was originated.
dst	The destination address for the update.
sport, dport	The source and destination ports for the update. (IPv6 RIP uses port 521, as shown in the display.)
command	The command field within the RIP packet. A value of 2 indicates that the RIP packet is a response (update); a value of 1 indicates that the RIP packet is a request.
version	The version of IPv6 RIP being used. The current version is 1.
mbz	There must be a 0 (mbz) field within the RIP packet.

Table 24 debug ipv6 rip Field Descriptions (continued)

Field	Description
#rte	Indicates the number of routing table entries (RTEs) the RIP packet contains.
tag metric prefix	The tag, metric, and prefix fields are specific to each RTE contained in the update. The tag field is intended to allow for the flagging of IPv6 RIP "internal" and "external" routes. The metric field is the distance metric from the router (sending this update) to the prefix. The prefix field is the IPv6 prefix of the destination being advertised.

Related Commands

Command	Description
debug ipv6 routing	Displays debug messages for IPv6 routing table updates and route cache updates.

debug ipv6 routing

To display debug messages for IPv6 routing table updates and route cache updates, use the **debug ipv6 routing** command in privileged EXEC mode. To disable debug messages for IPv6 routing table updates and route cache updates, use the **no** form of this command.

debug ipv6 routing

no debug ipv6 routing

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging for IPv6 routing table updates and route cache updates is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **debug ipv6 routing** command is similar to the **debug ip routing** command, except that it is IPv6-specific.

Note By default, the network server sends the output from debug commands and system error messages to the console. To redirect debug output, use the logging command options within global configuration mode. Destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. For complete information on debug commands and redirecting debug output, refer to the *Cisco IOS Debug Command Reference*.

Examples

The following example shows output for the **debug ipv6 routing** command:

```
Router# debug ipv6 routing

13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
13:18:43:IPv6RT0:Better next-hop for 2000:0:0:1:1::/80, [120/2]
13:19:09:IPv6RT0:Add 2000:0:0:2::/64 to table
```

```
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]
13:19:09:IPv6RT0:Add 2000:0:0:2:1::/80 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2:1::/80, [20/1]
13:19:09:IPv6RT0:Add 2000:0:0:4::/64 to table
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:4::/64, [20/1]
13:19:37:IPv6RT0:Add 2000:0:0:6::/64 to table
13:19:37:IPv6RT0:Better next-hop for 2000:0:0:6::/64, [20/2]
```

The **debug ipv6 routing** command displays messages whenever the routing table changes. For example, the following message indicates that a route to the prefix 2000:0:0:1:1::/80 was added to the routing table at the time specified in the message.

```
13:18:43:IPv6RT0:Add 2000:0:0:1:1::/80 to table
```

The following message indicates that the prefix 2000:0:0:2::/64 was already in the routing table; however, a received advertisement provided a lower cost path to the prefix. Therefore, the routing table was updated with the lower cost path. (The [20/1] in the example is the administrative distance [20] and metric [1] of the better path.)

```
13:19:09:IPv6RT0:Better next-hop for 2000:0:0:2::/64, [20/1]
```

Related Commands

Command	Description
debug ipv6 rip	Displays debug messages for IPv6 RIP routing transactions.

debug ipv6 snooping

To enable debugging for security snooping information in IPv6, use the **debug ipv6 snooping** command in privileged EXEC mode.

debug ipv6 snooping [**binding-table** | **classifier** | **errors** | **feature-manager** | **filter** *acl* | **ha** | **hw-api** | **interface** *interface* | **memory** | **ndp-inspection** | **policy** | **vlan** *vlanid* | **switcher** | **filter** *acl* | **interface** *interface* | *vlanid*]

no debug ipv6 snooping

Syntax Description

binding-table	(Optional) Displays information about the neighbor binding table.
classifier	(Optional) Displays information about the classifier.
errors	(Optional) Displays information about snooping security errors.
feature-manager	(Optional) Displays feature manager information.
filter *acl*	(Optional) Allows users to configure an access list to filter debugged traffic.
ha	(Optional) Displays information about high availability (HA) and stateful switchover (SSO).
hw-api	(Optional) Displays information about the hardware API.
interface *interface*	(Optional) Provides debugging information on a specified interface.
memory	(Optional) Displays information about security snooping memory.
ndp-inspection	(Optional) Displays information about Neighbor Discovery inspection.
policy	(Optional)
switcher	(Optional) Displays packets handled by the switcher.
vlanid	(Optional) Provides debugging information about a specified VLAN ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **debug ipv6 snooping** command provides debugging output for IPv6 snooping information.

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff.

Examples

The following example enables debugging for all IPv6 snooping information:

```
Router# debug ipv6 snooping
```

debug ipv6 snooping raguard

To enable debugging for security snooping information in the IPv6 router advertisement (RA) guard feature, use the **debug ipv6 snooping raguard** command in privileged EXEC mode.

debug ipv6 snooping raguard [*filter* | *interface* | *vlanid*]

no debug ipv6 snooping raguard

Syntax Description

filter	(Optional) Allows users to configure an access list to filter debugged traffic.
interface	(Optional) Provides debugging information on a specified interface configured with the IPv6 RA guard feature.
vlanid	(Optional) Provides debugging information about a specified VLAN ID configured with the IPv6 RA guard feature.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(54)SG	This command was introduced.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

The **debug ipv6 snooping raguard** command provides debugging output for IPv6 RA guard events and errors that may occur.

Because debugging output is assigned high priority in the CPU process, you should use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, you should use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

The following example enables debugging for the IPv6 RA guard feature:

```
Router# debug ipv6 snooping raguard
```

Related Commands

Command	Description
ipv6 nd raguard	Applies the IPv6 RA guard feature.

debug ipv6 spd

To enable debugging output for the most recent Selective Packet Discard (SPD) state transition, use the **debug ipv6 spd** command in privileged EXEC mode.

debug ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **debug ipv6 spd** command enables debugging information to be reviewed for the most recent SPD state transition and any trend historical data.

Examples

The following example shows how to enable debugging for the most recent SPD state transition:

```
Router# debug ipv6 spd
```

debug ipv6 static

To enable Bidirectional Forwarding Detection for IPv6 (BFDv6) debugging, use the **debug ipv6 static** command in privileged EXEC mode.

debug ipv6 static

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1.0	This command was introduced.
15.1(2)T	This command was modified. It was integrated into Cisco IOS Release 15.1(2)T.

Usage Guidelines

Use the **debug ipv6 static** command to monitor BFDv6 operation.

Examples

The following example enables BFDv6 debugging:

```
Router# debug ipv6 static
```

RelatedCommands

Command	Description
monitor event ipv6 static	Monitors the operation of the IPv6 static and IPv6 static BFDv6 neighbors using event trace.
show ipv6 static	Displays the current contents of the IPv6 routing table.

debug isis spf-events

To display a log of significant events during an Intermediate System-to-Intermediate System (IS-IS) shortest-path first (SPF) computation, use the **debug isis spf-events** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug isis spf-events

no debug isis spf-events

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(15)T	Support for IPv6 was added.
12.2(18)S	Support for IPv6 was added.
12.0(26)S	Support for IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

This command displays information about significant events that occur during SPF-related processing.

Examples

The following example displays significant events during an IS-IS SPF computation:

```
Router# debug isis spf-events

ISIS-Spf:  Compute L2 IPv6 SPT
ISIS-Spf: Move 0000.0000.1111.00-00 to PATHS, metric 0
ISIS-Spf: Add 0000.0000.2222.01-00 to TENT, metric 10
ISIS-Spf: Move 0000.0000.2222.01-00 to PATHS, metric 10
ISIS-Spf: considering adj to 0000.0000.2222 (Ethernet3/1) metric 10, level 2, circuit 3,
adj 3
ISIS-Spf:   (accepted)
ISIS-Spf: Add 0000.0000.2222.00-00 to TENT, metric 10
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.2222.00-00 to PATHS, metric 10
ISIS-Spf: Add 0000.0000.2222.02-00 to TENT, metric 20
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
```

```
ISIS-Spf: Move 0000.0000.2222.02-00 to PATHS, metric 20
ISIS-Spf: Add 0000.0000.3333.00-00 to TENT, metric 20
ISIS-Spf:   Next hop 0000.0000.2222 (Ethernet3/1)
ISIS-Spf: Move 0000.0000.3333.00-00 to PATHS, metric 20
```

debug nhrp

To enable Next Hop Resolution Protocol (NHRP) debugging, use the **debug nhrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp {**ipv4** | **ipv6**} [**cache** | **extension** | **packet** | **rate**]

no debug nhrp

Syntax Description(

ipv4	Specifies the IPv4 overlay address.
ipv6	Specifies the IPv6 overlay address.
cache	(Optional) Specifies NHRP cache operations.
extension	(Optional) Specifies NHRP extension processing.
packet	(Optional) Specifies NHRP activity.
rate	(Optional) Specifies NHRP rate limiting.

Command Default

NHRP debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows NHRP debugging output for IPv6:

```
Router# debug nhrp ipv6

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST
           - 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.
Aug  9 13:13:41.486: NHRP: Tunnel NBMA addr 11.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486: src: 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/32,
             dst: 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
```

The following example shows NHRP debugging output for IPv4:

```
Router# debug nhrp ipv4

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.  Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:       src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

Related Commands

Command	Description
debug dmvpn	Displays DMVPN session debugging information.
debug nhrp error	Displays NHRP error level debugging information.

debug nhrp condition

To enable Next Hop Resolution Protocol (NHRP) conditional debugging, use the **debug nhrp condition** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp condition [**interface tunnel** *number* | **peer** {**nbma** {*ip-address* | *FQDN-string*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*]

no debug nhrp condition [**interface tunnel** *number* | **peer** {**nbma** {*ip-address* | *FQDN-string*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*]

Syntax Description

tunnel	(Optional) Specifies a tunnel.
interface	(Optional) Displays NHRP information based on a specific interface.
tunnel *number*	(Optional) Specifies the tunnel address for the NHRP peer.
peer	(Optional) Specifies an NHRP peer.
nbma	(Optional) Specifies mapping nonbroadcast multiple access (NBMA).
ip-address	(Optional) The IPv4 address for the NHRP peer.
FQDN-string	(Optional) Next hop server (NHS) fully qualified domain name (FQDN) string.
ipv6-address	(Optional) The IPv6 address for the NHRP peer. **Note** Cisco IOS XE Release 2.5 does not support the *ipv6-address* argument.
vrf *vrf-name*	(Optional) Specifies debugging information for sessions related to the specified virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The *ipv6-address* argument was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.1(2)T	This command was modified. The *FQDN-string* argument was added.

Examples

The following example shows how to enable conditional NHRP debugging for a specified NBMA address:

```
Router# debug nhrp condition peer tunnel 192.0.2.1
```

The following example shows how to enable conditional NHRP debugging for a specified FQDN string:

```
Router# debug nhrp condition peer examplehub.example1.com
```

Related Commands

Command	Description
debug dmvpn	Displays DMVPN session debugging information.
debug nhrp error	Displays NHRP error level debugging information.

debug nhrp error

To display Next Hop Resolution Protocol (NHRP) error-level debugging information, use the **debug nhrp error** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp {**ipv4** | **ipv6**} **error**

no debug nhrp {**ipv4** | **ipv6**} **error**

Syntax Description

ipv4	Specifies the IPv6 overlay network.
ipv6	Specifies the IPv6 overlay network. **Note** Cisco IOS XE Release 2.5 does not support the **ipv6** keyword.

Command Default

NHRP error-level debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	The **ipv4** and **ipv6** keywords were added.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.

Examples

The following example shows how to enable error level debugging for IPv4 NHRP:

```
Router# debug nhrp ipv4 error

NHRP errors debugging is on
```

Related Commands

Command	Description
debug dmvpn	Displays DMVPN session debugging information.
debug nhrp condition	Enables NHRP conditional debugging.

debug ntp

To display debugging messages for Network Time Protocol (NTP) features, use the **debug ntp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ntp {**adjust** | **all** | **authentication** | **core** | **events** | **loopfilter** | **packet** | **params** | **refclock** | **select** | **sync** | **validity**}

no debug ntp {**adjust** | **all** | **authentication** | **core** | **events** | **loopfilter** | **packet** | **params** | **refclock** | **select** | **sync** | **validity**}

Syntax Description

adjust	Displays debugging information on NTP clock adjustments.
all	Displays all debugging information on NTP.
authentication	Displays debugging information on NTP authentication.
core	Displays debugging information on NTP core messages.
events	Displays debugging information on NTP events.
loopfilter	Displays debugging information on NTP loop filters.
packet	Displays debugging information on NTP packets.
params	Displays debugging information on NTP clock parameters.
refclock	Displays debugging information on NTP reference clocks.
select	Displays debugging information on NTP clock selection.
sync	Displays debugging information on NTP clock synchronization.
validity	Displays debugging information on NTP peer clock validity.

Command Default

Debugging is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1	This command was introduced in a release prior to Cisco IOS Release 12.1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	Support for IPv6 and NTP version 4 was added. The **all** and **core** keywords were added. The **authentication**, **loopfilter**, **params**, **select**, **sync** and **validity** keywords were removed. The **packets** keyword was modified as **packet**.

Usage Guidelines

Starting from Cisco IOS Release 12.4(20)T, NTP version 4 is supported. In NTP version 4 the debugging options available are **adjust**, **all**, **core**, **events**, **packet**, and **refclock**. In NTP version 3 the debugging options available were **events**, **authentication**, **loopfilter**, **packets**, **params**, **select**, **sync** and **validity**.

Examples

The following example shows how to enable all debugging options for NTP:

```
Router# debug ntp all

NTP events debugging is on
NTP core messages debugging is on
NTP clock adjustments debugging is on
NTP reference clocks debugging is on
NTP packets debugging is on
```

Related Commands

Command	Description
ntp refclock	Configures an external clock source for use with NTP services.

debug ospfv3

To display debugging information for Open Shortest Path First version 3 (OSPF) for IPv4 and IPv6, use the **debug ospfv3** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] [**adj** | **ipsec** | **database-timer** | **flood** | **hello** | **lsa-generation** | **retransmission**]

no debug ospfv3 [*process-id*] [*address-family*] [**adj** | **ipsec** | **database-timer** | **flood** | **hello** | **lsa-generation** | **retransmission**]

Syntax Description

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
adj	(Optional) Displays adjacency information.
ipsec	(Optional) Displays the interaction between OSPFv3 and IPSec, including creation and removal of policy definitions.
database-timer	(Optional) Displays database-timer information.
flood	(Optional) Displays flooding information.
hello	(Optional) Displays hello packet information.
l2api	(Optional) Enables layer 2 and layer 3 application program interface (API) debugging.
lsa-generation	(Optional) Displays link-state advertisement (LSA) generation information for all LSA types.
retransmission	(Optional) Displays retransmission information.

Command Default

Debugging of OSPFv3 is not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays adjacency information for OSPFv3:

```
Router# debug ospfv3 adj
```

debug ospfv3 database-timer rate-limit

To display debugging information about the current wait-time used for shortest path first (SPF) scheduling, use the **debug ospfv3 database-timer rate-limit** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **database-timer rate-limit** [*acl-number*]

no debug ospfv3 [*process-id*] [*address-family*] **database-timer rate-limit**

SyntaxDescription

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.
acl-number	(Optional) Access list number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example shows how to turn on debugging for SPF scheduling in OSPFv3 process 1:

```
Router# debug ospfv3 1 database-timer rate-limit
```

debug ospfv3 events

To display information on Open Shortest Path First version 3 (OSPFv3)-related events, such as designated router selection and shortest path first (SPF) calculation, use the **debug ospfv3 events** command in privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **events**

no debug ipv6 ospfv3 [*process-id*] [*address-family*] **events**

SyntaxDescription

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information on OSPFv3-related events:

```
Router# debug ospfv3 events
```

debug ospfv3 lsdb

To display database modifications for Open Shortest Path First version 3 (OSPFv3), use the **debug ospfv3 lsdb** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **lsdb**

no debug ospfv3 [*process-id*] [*address-family*] **lsdb**

SyntaxDescription

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays database modification information for OSPFv3:

```
Router# debug ospfv3 lsdb
```

debug ospfv3 packet

To display information about each Open Shortest Path First version 3 (OSPFv3) packet received, use the **debug ospfv3 packet** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ospfv3 [*process-id*] [*address-family*] **packet**

no debug ospfv3 [*process-id*] [*address-family*] **packet**

SyntaxDescription

process-id	(Optional) Internal identification. The number used here is the number assigned administratively when enabling the OSPFv3 routing process and can be a value from 1 through 65535.
address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Consult Cisco technical support before using this command.

Examples

The following example displays information about each OSPFv3 packet received:

```
Router# debug ospfv3 packet
```

debug ospfv3 spf statistic

To display statistical information while running the shortest path first (SPF) algorithm, use the **debug ospfv3 spf statistic** command in privileged EXEC mode. To disable the debugging output, use the **no** form of this command.

debug ospfv3 [*address-family*] **spf statistic**

no debug ospfv3 [*address-family*] **spf statistic**

SyntaxDescription

address-family	(Optional) Enter **ipv6** for the IPv6 address family or **ipv4** for the IPv4 address family.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The **debug ospfv3 spf statistic** command displays the SPF calculation times in milliseconds, the node count, and a time stamp. Consult Cisco technical support before using this command.

Examples

The following example displays statistical information while running the SPF algorithm:

```
Router# debug ospfv3 spf statistics
```

Related Commands

Command	Description
debug ospfv3	Displays debugging information for the OSPFv3 feature.
debug ospfv3 events	Displays information on OSPFv3-related events.
debug ospfv3 packet	Displays information about each OSPFv3 packet received.

debug ppp unique address

To display debugging information about duplicate addresses received from RADIUS, use the **debug ppp unique address** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ipv6 policy

no debug ipv6 policy

Syntax Description

This command has no arguments or keywords.

Command Default

Information about duplicate addresses received from RADIUS is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **debug ppp unique address** command enables you to view debugging information about duplicate addresses received from RADIUS.

Examples

The following example enables debugging output about duplicate addresses received from RADIUS:

```
Router# debug ppp unique address
```

default (IPv6 OSPF)

To return a parameter to its default value, use the **default** command in router configuration mode.

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

Syntax Description

area	(Optional) Open Shortest Path First (OSPF) for IPv6 area parameters.
auto-cost	(Optional) OSPF interface cost according to bandwidth.
default-information	(Optional) Distributes default information.
default-metric	(Optional) Metric for a redistributed route.
discard-route	(Optional) Enables or disables discard-route installation.
distance	(Optional) Administrative distance.
distribute-list	(Optional) Filter networks in routing updates.
ignore	(Optional) Ignores a specific event.
log-adjacency-changes	(Optional) Log changes in the adjacency state.
maximum-paths	(Optional) Forwards packets over multiple paths.
passive-interface	(Optional) Suppresses routing updates on an interface.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
router-id	(Optional) Router ID for the specified routing process.
summary-prefix	(Optional) OSPF summary prefix.
timers	(Optional) OSPF timers.

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The command is removed if it is disabled by default.

Examples

In the following example, OSPF for IPv6 area parameters are reset to the default values:

```
default timers spf
```

default (OSPFv3)

To return an Open Shortest Path First version 3 (OSPFv3) parameter to its default value, use the **default** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode.

default {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]

Syntax Description

area	OSPFv3 area parameters.
area-ID	Area ID associated with the OSPFv3 interface.
range	Summarizes routes that match the address or address mask on border routers only.
ipv6-prefix	An IPv6 address.
virtual-link	Defines a virtual link and its parameters.s
router-id	Router ID associated with the virtual-link neighbor.
default-information originate	(Optional) Distribution of default route information.
always	(Optional) Always provides the default route information.
metric	(Optional) Provides the OSPFv3 default metric.
metric-type	(Optional) Provides the OSPFv3 metric type for default routes.
route-map	(Optional) Provides the route-map reference.
distance	(Optional) Provides the administrative distance.
distribute-list	(Optional) Filter networks in routing updates.
prefix-list *prefix-list-name*	Filters connections based on an IPv6 prefix list.
in	Filters incoming routing updates.
out	Filters outgoing routing updates.
interface	(Optional) Filters incoming or outgoing routing updates on a specified interface.
maximum-paths	(Optional) Forwards packets over multiple paths.
paths	Maximum number of paths. The range is from 1 through 32.
redistribute	(Optional) Redistributes IPv6 prefixes from another routing protocol.
protocol	The routing protocol from which IPv6 prefixes are redistributed.
summary-prefix	(Optional) OSPFv3 summary prefix.

Command Default

This command is disabled by default.

Command Modes

OSPFv3 router configuration mode (config-router)
IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Use the **default** command in OSPFv3 router configuration mode to reset OSPFv3 parameters for an IPv4 OSPFv3 process.

Use the **default** command in IPv6 or IPv4 address family configuration mode to reset OSPFv3 parameters for an IPv6 or an IPv4 process.

Examples

In the following example, OSPFv3 parameters are reset to the default value for area 1 in IPv6 address family configuration mode:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# default area 1
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

default-information originate (IPv6 IS-IS)

To inject an IPv6 default route into an Intermediate System-to-Intermediate System (IS-IS) IPv6 routing domain, use the **default-information originate** command in address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *map-name*]

no default-information originate [**route-map** *map-name*]

Syntax Description

route-map *map-name*	(Optional) Route map should be used to advertise the default route conditionally. The *map-name* argument identifies a configured route map.

Command Default

This feature is disabled.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **default-information originate** (IPv6 IS-IS) command is similar to the **default-information originate** (IS-IS) command, except that it is IPv6-specific.

If a router configured with this command has an IPv6 route to ::/0 in the routing table, IS-IS will originate an advertisement for ::/0 in its link-state packets (LSPs).

Without a route map, the default is advertised only in Level 2 LSPs. For Level 1 routing, there is another mechanism to find the default route, which is for the router to look for the closest Level 1 or Level 2 router. The closest Level 1 or Level 2 router can be found by looking at the attached bit (ATT) in Level 1 LSPs.

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.

- Advertise ::/0 conditionally.

With a **match ipv6 address** *standard-access-list* command, you can specify one or more IPv6 routes that must exist before the router will advertise ::/0.

Examples

The following example shows the IPv6 default route (::/0) being advertised with all other routes in router updates:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# default-information originate
```

Related Commands

Command	Description
address-family ipv6 (IS-IS)	Specifies the IPv6 address family and places the router in address family configuration mode.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
show isis database	Displays the IS-IS link-state database.

default-information originate (OSPFv3)

To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) for a routing domain, use the **default-information originate** command in IPv6 or IPv4 address family configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*]

no default-information originate [**always** | **metric** *metric-value* | **metric-type** *type-value* | **route-map** *map-name*]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric *metric-value*	(Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the **default-metric** router configuration command, the default metric value is 10. The default metric value range is from 0 to 16777214.
metric-type *type-value*	(Optional) External link type associated with the default route advertised into the OSPF for IPv6 routing domain. It can be one of the following values: **1**—Type 1 external route **2**—Type 2 external route The default is type 2 external route.
route-map *map-name*	(Optional) Routing process will generate the default route if the route map is satisfied.

Command Default

This command is disabled by default.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Whenever you use the **redistribute** or the **default-information** command to redistribute routes into an OSPFv3 routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF for IPv6 routing domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

When you use this command for the OSPFv3 process, the default network must reside in the routing table, and you must satisfy the **route-map** *map-name* keyword and argument. Use the **default-information originate always route-map** *map-name* form of the command when you do not want the dependency on the default network in the routing table.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPFv3 routing domain, an external metric type of type 2, and the default route to be always advertised:

```
Router(config-router-af)# default-information originate always metric 100 metric-type 2
```

default-metric (EIGRP)

To set metrics for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **default-metric** command in router configuration mode or address-family topology configuration mode. To remove the metric value and restore the default state, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

bandwidth	Minimum bandwidth of the route in kilobytes per second. It can be from 1 to 4294967295.
delay	Route delay in tens of microseconds. It can be 1 or any positive number that is a multiple of 39.1 nanoseconds.
reliability	Likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
mtu	The smallest allowed value for the maximum transmission unit (MTU), expressed in bytes. It can be from 1 to 65535.

Command Default

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

Command Modes

Router configuration (config-router)
Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	Address family support was added.
12.2(15)T	Address family support was added.
12.2(18)S	Address family support was added.
12.4(6)T	Support for IPv6 was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family topology configuration mode was added. This command must be entered in address-family topology configuration mode when EIGRP is configured with a named router configuration.

Release	Modification
12.2(33)SRE	This command was modified. Address-family topology configuration mode was added. This command must be entered in address-family topology configuration mode when EIGRP is configured with a named router configuration.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

You must use a default metric to redistribute a protocol into EIGRP, unless you use the **redistribute** command.

Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

Default metrics are supported only when you are redistributing from EIGRP or static routes.

Examples

The following example shows how the redistributed Routing Information Protocol (RIP) metrics are translated into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500:

```
Router(config)# router eigrp 109
Router(config-router)# network 172.16.0.0
Router(config-router)# redistribute rip
Router(config-router)# default-metric 1000 100 250 100 1500
```

The following example shows how the redistributed EIGRP service family 6473 metrics are translated into EIGRP metric with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# af-interface default
Router(config-router-af-interface)# no shutdown
Router(config-router-af-interface)# exit
Router(config-router-af)# topology base
Router(config-router-af-topology)# default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
af-interface	Enters address-family interface configuration mode to configure interface-specific EIGRP commands.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

Command	Description
router eigrp	Configures the EIGRP address-family process.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters router address-family topology configuration mode.

default-metric (OSPFv3)

To set default metric values for IPv4 and IPv6 routes redistributed into the Open Shortest Path First version 3 (OSPFv3) routing protocol, use the **default-metric** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To return to the default state, use the **no** form of this command.

default-metric *metric-value*

no default-metric *metric-value*

Syntax Description

metric-value	Default metric value appropriate for the specified routing protocol. The range is from 1 to 4294967295.

Command Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Modes

OSPFv3 router configuration mode (config-router)
IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Finer control over the metrics of redistributed routes can be gained by using the options to the **redistribute** command, including route maps.

Examples

The following example shows how to enter IPv6 AF and configure OSPFv3 routing protocol redistributing routes from the OSPFv3 process named process1. All the redistributed routes are advertised with a metric of 10.

```
router ospfv3 100
 address-family ipv6 unicast
 default-metric 10
 redistribute ospfv3 process1
```

The following example shows an OSPFv3 routing protocol redistributing routes from the OSPFv3 process named process1. All the redistributed routes are advertised with a metric of 10.

```
ipv6 router ospf 100
 default-metric 10
 redistribute ospfv3 process1
```

Related Commands

Command	Description
redistribute (OSPFv3)	Redistributes IPv6 and IPv4 routes from one routing domain into another routing domain.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

no deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]

Internet Control Message Protocol

deny icmp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*] | *icmp-message*] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

deny tcp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**ack**] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**established**] [**fin**] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**psh**] [**range** {*port* | *protocol*}] [**routing**] [**routing-type** *routing-number*] [**rst**] [**sequence** *value*] [**syn**] [**time-range** *name*] [**urg**]

User Datagram Protocol

deny udp {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set deny conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix/prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6-prefix/prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/prefix-length	The destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set deny conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
auth	Allows matching traffic against the presence of the authentication header in combination with the specified protocol; that is, TCP or UDP.
dest-option-type	(Optional) Matches IPv6 packets against the destination option extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.

flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(Optional) Extension header type. Allows matching of any IPv6 packet including a mobility header, regardless of the value of the mobility-header-type field within that header.
mobility-type	(Optional) Mobility header type. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Name of a mobility header type. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Allows routing headers with a value in the type field to be matched independently. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header

sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
undetermined-transport	(Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **deny** (IPv6) command is similar to the **deny** (IP) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By 1default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.

The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix*/*prefix-length* and *destination-ipv6-prefix*/*prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on Ethernet interface 0. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of Ethernet interface 0. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of Ethernet interface 0. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of Ethernet interface 0. The second permit entry in the list permits all other traffic to exit out of Ethernet interface 0. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any

interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

The following example shows how to allow TCP or UDP parsing although an IPsec AH is present:

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

destination-pattern

To specify either the prefix or the full E.164 telephone number to be used for a dial peer, use the **destination-pattern** command in dial peer configuration mode. To disable the configured prefix or telephone number, use the **no** form of this command.

destination-pattern [**+**]*string*[**T**]

no destination-pattern [**+**]*string*[**T**]

Syntax Description

+	(Optional) Character that indicates an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: • The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. • Comma (,), which inserts a pause between digits. • Period (.), which matches any entered digit (this character is used as a wildcard). • Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. • Plus sign (+), which indicates that the preceding digit occurred one or more times. **Note** The plus sign used as part of a digit string is different from the plus sign that can be used preceding a digit string to indicate that the string is an E.164 standard number. • Circumflex (^), which indicates a match to the beginning of the string. • Dollar sign ($), which matches the null string at the end of the input string. • Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). • Question mark (?), which indicates that the preceding digit occurred zero or one time. • Brackets ([ ]), which indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range. • Parentheses (( )), which indicate a pattern and are the same as the regular expression rule.
T	(Optional) Control character that indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Command Default

The command is enabled with a null string.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.1(1)	The command was integrated into Cisco IOS Release 12.1(1).
12.0(7)XR	This command was implemented on the Cisco AS5300 and modified to support the plus sign, percent sign, question mark, brackets, and parentheses symbols in the dial string.
12.0(7)XK	This command was modified. Support for the plus sign, percent sign, question mark, brackets, and parentheses in the dial string was added to the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T and implemented on the Cisco 1750, Cisco 7200 series, and Cisco 7500 series. The modifications for the Cisco MC3810 in Cisco IOS Release12.0(7)XK are not supported in this release.
12.1(2)T	The modifications made in Cisco IOS Release 12.0(7)XK for the Cisco MC3810 were integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series and Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, the Cisco ICS7750, and the Cisco VG200.
12.4(22)T	Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use the **destination-pattern** command to define the E.164 telephone number for a dial peer.

The pattern you configure is used to match dialed digits to a dial peer. The dial peer is then used to complete the call. When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number configured as the destination pattern for the voice-telephony peer. The router then strips out the left-justified numbers that correspond to the destination pattern. If you have configured a prefix, the prefix is prepended to the remaining numbers, creating a dial string that the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

There are areas in the world (for example, certain European countries) where valid telephone numbers can vary in length. Use the optional control character **T** to indicate that a particular **destination-pattern** value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired.

Note Cisco IOS software does not verify the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Examples

The following example shows configuration of the E.164 telephone number 555-0179 for a dial peer:

```
dial-peer voice 10 pots
 destination-pattern +5550179
```

The following example shows configuration of a destination pattern in which the pattern "43" is repeated multiple times preceding the digits "555":

```
dial-peer voice 1 voip
 destination-pattern 555(43)+
```

The following example shows configuration of a destination pattern in which the preceding digit pattern is repeated multiple times:

```
dial-peer voice 2 voip
 destination-pattern 555%
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550109 and 5550199:

```
dial-peer voice 3 vofr
 destination-pattern 55501[0-9]9
```

The following example shows configuration of a destination pattern in which the possible numeric values are between 5550439, 5553439, 5555439, 5557439, and 5559439:

```
dial-peer voice 4 voatm
 destination-pattern 555[03579]439
```

The following example shows configuration of a destination pattern in which the digit-by-digit matching is prevented and the entire string is received:

```
dial-peer voice 2 voip
 destination-pattern 555T
```

Related Commands

Command	Description
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
dial-peer terminator	Designates a special character to be used as a terminator for variable-length dialed numbers.
incoming called-number (dial peer)	Specifies a digit string that can be matched by an incoming call to associate that call with a dial peer.
prefix	Specifies the prefix of the dialed digits for a dial peer.
timeouts interdigit	Configures the interdigit timeout value for a specified voice port.

device-role

To specify the role of the device attached to the port, use the **device-role** command in Neighbor Discovery (ND) inspection policy configuration mode or Router Advertisement (RA) guard policy configuration mode.

device-role {**host** | **monitor** | **router**}

SyntaxDescription

host	Sets the role of the device to host.
monitor	Sets the role of the device to monitor.
router	Sets the role of the device to router.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], RA, or redirect) are allowed on this port.

When the **router** or **monitor** keywords are used, the multicast RS are bridged on the port, regardless of whether limited broadcast is enabled. However, the **monitor** keyword does not allow inbound RA or redirect messages. When the **monitor** keyword is used, devices that need these messages will receive them.

Examples

The following example defines an NDP policy name as policy1, places the router in ND inspection policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host
```

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

dial-peer voice

To define a particular dial peer, to specify the method of voice encapsulation, and to enter dial peer configuration mode, use the **dial-peer voice** command in global configuration mode. To delete a defined dial peer, use the **no** form of this command.

Cisco 1750 and Cisco 1751 Modular Access Routers

dial-peer voice *tag* {**pots** | **vofr** | **voip system**}

no dial-peer voice *tag* {**pots** | **vofr** | **voip system**}

Cisco 2600 Series, Cisco 2600XM, Cisco 3600 Series, Cisco 3700 Series, Cisco 7204VXR and Cisco 7206VXR

dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip system**}

no dial-peer voice *tag* {**pots** | **voatm** | **vofr** | **voip system**}

Cisco 7200 Series

dial-peer voice *tag* **vofr**

no dial-peer voice *tag* **vofr**

Cisco AS5300

dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip system**}

no dial-peer voice *tag* {**mmoip** | **pots** | **vofr** | **voip system**}

Syntax Description

tag	Digits that define a particular dial peer. Range is from 1 to 2147483647.
pots	Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone.
vofr	Specifies that this is a Voice over Frame Relay (VoFR) dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network.
voip	Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.
system	Indicates that this is a system that uses VoIP.
voatm	Specifies that this is a Voice over ATM (VoATM) dial peer that uses real-time ATM adaptation layer 5 (AAL5) voice encapsulation on the ATM backbone network.
mmoip	Indicates that this is a multimedia mail peer that uses IP encapsulation on the IP backbone.

Command Default

No dial peer is defined.
No method of voice encapsulation is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was implemented on the Cisco MC3810, with support for the **pots**, **voatm**, **vofr**, and **vohdlc** keywords.
12.0(3)T	This command was implemented on the Cisco AS5300, with support for the **pots** and **voip** keywords.
12.0(3)XG	The **vofr** keyword was added for the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	The **vofr** keyword was added for the Cisco 7200 series.
12.0(4)XJ	The **mmoip** keyword was added for the Cisco AS5300. The **dial-peer voice** command was implemented for store-and-forward fax.
12.0(7)XK	The **voip** keyword was added for the Cisco MC3810, and the **voatm** keyword was added for the Cisco 3600 series. Support for the **vohdlc** keyword on the Cisco MC3810 was removed.
12.1(1)	The **mmoip** keyword addition in Cisco IOS Release 12.0(4)XJ was integrated into Cisco IOS Release 12.1(1). The **dial-peer voice** implementation for store-and-forward fax was integrated into Cisco IOS Release 12.1(1).
12.1(2)T	The keyword changes in Cisco IOS Release 12.0(7)XK were integrated into Cisco IOS Release 12.1(2)T.
12.1(5)T	This command was implemented on the Cisco AS5300 and integrated into Cisco IOS Release 12.1(5)T.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XN	Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. This command was implemented on the Cisco IAD2420 series.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented on the Cisco 2600XM, Cisco ICS7750, and Cisco VG200.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

Use the **dial-peer voice** global configuration command to switch to dial peer configuration mode from global configuration mode and to define a particular dial peer. Use the **exit** command to exit dial peer configuration mode and return to global configuration mode.

A newly created dial peer remains defined and active until you delete it with the **no** form of the **dial-peer voice** command. To disable a dial peer, use the **no shutdown** command in dial peer configuration mode.

In store-and-forward fax on the Cisco AS5300, the POTS dial peer defines the inbound faxing line characteristics from the sending fax device to the receiving Cisco AS5300 and the outbound line characteristics from the sending Cisco AS5300 to the receiving fax device. The Multimedia Mail over Internet Protocol (MMoIP) dial peer defines the inbound faxing line characteristics from the Cisco AS5300 to the receiving Simple Mail Transfer Protocol (SMTP) mail server. This command works with both on-ramp and off-ramp store-and-forward fax functions.

Note On the Cisco AS5300, MMoIP is available only if you have modem ISDN channel aggregation (MICA) technologies modems.

Examples

The following example shows how to access dial peer configuration mode and configure a POTS peer identified as dial peer 10 and an MMoIP dial peer identified as dial peer 20:

```
dial-peer voice 10 pots
dial-peer voice 20 mmoip
```

The following example deletes the MMoIP peer identified as dial peer 20:

```
no dial-peer voice 20 mmoip
```

The following example shows how the **dial-peer voice** command is used to configure the extended echo canceller. In this instance, **pots** indicates that this is a POTS peer using VoIP encapsulation on the IP backbone, and it uses the unique numeric identifier tag 133001.

```
Router(config)# dial-peer voice 133001 pots
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a VoFR dial peer.
destination-pattern	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP for VoFR applications.
session protocol	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
shutdown	Changes the administrative state of the selected dial peer from up to down.

dialer-group

To control access by configuring an interface to belong to a specific dialing group, use the **dialer-group** command in interface configuration mode. To remove an interface from the specified dialer access group, use the **no** form of this command.

dialer-group *group-number*

no dialer-group

Syntax Description

group-number	Number of the dialer access group to which the specific interface belongs. This access group is defined with the **dialer-list** command. Acceptable values are nonzero, positive integers between 1 and 10.

Defaults

No access is predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	Support for IPv6 was added.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

An interface can be associated with a single dialer access group only; multiple **dialer-group** assignment is not allowed. A second dialer access group assignment will override the first. A dialer access group is defined with the **dialer-group** command. The **dialer-list** command associates an access list with a dialer access group.

Packets that match the dialer group specified trigger a connection request.

Examples

The following example specifies dialer access group number 1.

The destination address of the packet is evaluated against the access list specified in the associated **dialer-list** command. If it passes, either a call is initiated (if no connection has already been established) or the idle timer is reset (if a call is currently connected).

```
interface async 1
 dialer-group 1
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 protocol ip list 101
```

Related Commands

Command	Description
dialer-list protocol (Dial)	Defines a DDR dialer list to control dialing by protocol or by a combination of protocol and an access list.

dialer-list protocol

To define a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list, use the **dialer-list protocol** command in global configuration mode. To delete a dialer list, use the **no** form of this command.

dialer-list *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

no dialer-list *dialer-group* [**protocol** *protocol-name* [**list** *access-list-number* | *access-group*]]

Syntax Description

dialer-group	Number of a dialer access group identified in any **dialer-group** interface configuration command.
protocol-name	One of the following protocol keywords: **appletalk**, **bridge**, **clns**, **clns_es**, **clns_is**, **decnet**, **decnet_router-L1**, **decnet_router-L2**, **decnet_node**, **ip**, **ipx**, **ipv6**, **vines**, or **xns**.
permit	Permits access to an entire protocol.
deny	Denies access to an entire protocol.
list	Specifies that an access list will be used for defining a granularity finer than an entire protocol.
access-list-number	Access list numbers specified in any DECnet, Banyan VINES, IP, Novell IPX, or XNS standard or extended access lists, including Novell IPX extended service access point (SAP) access lists and bridging types, and IPv6 access lists. See Table 25 for the supported access list types and numbers.
access-group	Filter list name used in the **clns filter-set** and **clns access-group** commands.

Command Default

No dialer lists are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keyword and arguments were added: • **list** • *access-list-number* and *access-group*
12.2(2)T	The **ipv6** keyword was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The various **no** forms of this command have the following effects:

- The **no dialer-list 1** command deletes all lists configured with list 1, regardless of the keyword previously used (**permit**, **deny**, **protocol**, or **list**).
- The **no dialer-list 1 protocol** *protocol-name* command deletes all lists configured with list 1 and **protocol** *protocol-name*.
- The **no dialer-list 1 protocol** *protocol-name* **list** *access-list-number* command deletes the specified list.

The **dialer-list protocol** command permits or denies access to an entire protocol. The **dialer-list protocol list** command provides a finer permission granularity and also supports protocols that were not previously supported.

The **dialer-list protocol list** command applies protocol access lists to dialer access groups to control dialing using DDR. The dialer access groups are defined with the **dialer-group** command.

Table 25 lists the access list types and number range that the **dialer-list protocol list** command supports. The table does not include International Organization for Standardization (ISO) Connectionless Network Services (CLNS) or IPv6 because those protocols use filter names instead of predefined access list numbers.

Table 25 dialer-list protocol Command Supported Access List Types and Number Range

Access List Type	Access List Number Range (Decimal)
AppleTalk	600 to 699
Banyan VINES (standard)	1 to 100
Banyan VINES (extended)	101 to 200
DECnet	300 to 399
IP (standard)	1 to 99
IP (extended)	100 to 199
Novell IPX (standard)	800 to 899
Novell IPX (extended)	900 to 999
Transparent Bridging	200 to 299
XNS	500 to 599

Examples

Dialing occurs when an interesting packet (one that matches access list specifications) needs to be output on an interface. Using the standard access list method, packets can be classified as interesting or uninteresting. In the following example, Integrated Gateway Routing Protocol (IGRP) TCP/IP routing protocol updates are not classified as interesting and do not initiate calls:

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
```

The following example classifies all other IP packets as interesting and permits them to initiate calls:

```
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Then the following command places list 101 into dialer access group 1:

```
dialer-list 1 protocol ip list 101
```

In the following example, DECnet access lists allow any DECnet packets with source area 10 and destination area 20 to trigger calls:

```
access-list 301 permit 10.0 0.1023 10.0 0.1023
access-list 301 permit 10.0 0.1023 20.0 0.1023
```

Then the following command places access list 301 into dialer access group 1:

```
dialer-list 1 protocol decnet list 301
```

In the following example, both IP and VINES access lists are defined. The IP access lists define IGRP packets as uninteresting, but permits all other IP packets to trigger calls. The VINES access lists do not allow Routing Table Protocol (RTP) routing updates to trigger calls, but allow any other data packets to trigger calls.

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
vines access-list 107 deny RTP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
vines access-list 107 permit IP 00000000:0000 FFFFFFFF:FFFF 00000000:0000 FFFFFFFF:FFFF
```

Then the following two commands place the IP and VINES access lists into dialer access group 1:

```
dialer-list 1 protocol ip list 101
dialer-list 1 protocol vines list 107
```

In the following example, a CLNS filter is defined and then the filter is placed in dialer access group 1:

```
clns filter-set ddrline permit 47.0004.0001....
!
dialer-list 1 protocol clns list ddrline
```

The following example configures an IPv6 access list named list2 and places the access list in dialer access group 1:

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any
!
dialer-list 1 protocol ipv6 list list2
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
clns filter-set	Builds a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions.
dialer-group	Controls access by configuring an interface to belong to a specific dialing group.

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
vines access-list	Creates a VINES access list.

discard-route (IPv6)

To reinstall either an external or internal discard route that was previously removed, use the **discard-route** command in router configuration mode. To remove either an external or internal discard route, use the **no** form of this command.

discard-route [**external** | **internal**]

no discard-route [**external** | **internal**]

Syntax Description

external	(Optional) Reinstalls the discard route entry for redistributed summarized routes on an Autonomous System Boundary Router (ASBR).
internal	(Optional) Reinstalls the discard-route entry for summarized internal routes on the Area Border Router (ABR).

Command Default

External and internal discard route entries are installed.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

External and internal discard route entries are installed in routing tables by default. During route summarization, routing loops may occur when data is sent to a nonexisting network that appears to be a part of the summary, and the router performing the summarization has a less specific route (pointing back to the sending router) for this network in its routing table. To prevent the routing loop, a discard route entry is installed in the routing table of the ABR or ASBR.

If for any reason you do not want to use the external or internal discard route, remove the discard route by entering the **no discard-route** command with either the **external** or **internal** keyword.

Examples

The following display shows the discard route functionality installed by default. When external or internal routes are summarized, a summary route to Null0 will appear in the router output from the **show ipv6 route** command. See the router output lines that appear in bold font:

```
Router# show ipv6 route

IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
C   2001:0:11::/64 [0/0]
     via ::, Ethernet0/0
L   2001:0:11:0:A8BB:CCFF:FE00:6600/128 [0/0]
     via ::, Ethernet0/0
C   2001:1:1::/64 [0/0]
     via ::, Ethernet1/0
L   2001:1:1:0:A8BB:CCFF:FE00:6601/128 [0/0]
     via ::, Ethernet1/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0

Router# show ipv6 route ospf

IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
```

When the **no discard-route** command with the **internal** keyword is entered, notice the following route change, indicated by the router output lines that appear in bold font:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipv6 router ospf 1
Router(config-router)# no discard-route internal
Router(config-router)# end

Router# show ipv6 route ospf

IPv6 Routing Table - 6 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

Next, the **no discard-route** command with the **external** keyword is entered to remove the external discard route entry:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config-router)# no discard-route external
Router(config-router)# end
```

The following router output from the **show running-config** command confirms that both the external and internal discard routes have been removed from the routing table. See the router output lines that appear in bold font:

```
Router# show running-config

Building configuration...

Current configuration :2490 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
logging buffered 20480 debugging
logging console warnings
!
clock timezone PST -8
clock summer-time PDT recurring
no aaa new-model
ip subnet-zero
no ip domain lookup
!
!
ip audit po max-events 100
ipv6 unicast-routing
no ftp-server write-enable
!
.
.
.
interface Ethernet0/0
 no ip address
 ipv6 address 2001:0:11::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 0
 no cdp enable
!
interface Ethernet1/0
 no ip address
 ipv6 address 2001:1:1::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
 no cdp enable
  .
  .
  .
```

```
ipv6 router ospf 1
 router-id 2.0.0.1
 log-adjacency-changes
 no discard-route external
 no discard-route internal
 area 0 range 2001::/32
 redistribute rip 1
!
```

Related Commands

Command	Description
show ipv6 route	Displays the current contents of the IPv6 routing table.
show running config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

distance (IPv6)

To configure an administrative distance for Intermediate System-to-Intermediate System (IS-IS), Routing Information Protocol (RIP), or Open Shortest Path First (OSPF) IPv6 routes inserted into the IPv6 routing table, use the **distance** command in address family configuration or router configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

no distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

Syntax Description

ospf	(Optional) Administrative distance for OSPF for IPv6 routes.
external	External type 5 and type 7 routes for OSPF for IPv6 routes.
inter-area	Inter-area routes for OSPF for IPv6 routes.
intra-area	Intra-area routes for OSPF for IPv6 routes.
distance	The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)

Command Default

IS-IS: 115
RIP: 120
OSPF for IPv6: 110

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was implemented on the Cisco 12000 series Internet routers, and support for IS-IS was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	OSPF for IPv6 information was added. The **external**, **inter-area**, and **intra-area** keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.4	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **distance** (IPv6) command is similar to the **distance** (IP) command, except that it is IPv6-specific.

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 190 for the IPv6 IS-IS routing process named area01:

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# distance 190
```

The following example configures an administrative distance of 200 for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-router)# distance 200
```

The following example configures an administrative distance of 200 for external type 5 and type 7 routes for OSPF for IPv6:

```
Router(config)# ipv6 router ospf
Router(config-router)# distance ospf external 200
```

distance (IPv6 EIGRP)

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance** command in router configuration mode. To reset these values to their defaults, use the **no** form of this command.

distance *internal-distance external-distance*

no distance

Syntax Description

internal-distance	Administrative distance for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6 internal routes. Internal routes are those that are learned from another entity within the same autonomous system. The distance can be a value from 1 to 255.
external-distance	Administrative distance for EIGRP for IPv6 external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. The distance can be a value from 1 to 255.

Command Default

internal-distance: 90
external-distance: 170

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Use the **distance** command if another protocol is known to be able to provide a better route to a node than was actually learned via external EIGRP for IPv6, or if some internal routes should be preferred by EIGRP for IPv6.

Table 26 lists the default administrative distances.

Table 26 Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1

Table 26 Default Administrative Distances (continued)

Route Source	Default Distance
EIGRP summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
Open Shortest Path First (OSPF)	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
EIGRP external route	170
Internal BGP	200
Unknown	255

Examples

The following example sets the internal distance to 95 and the external distance to 165:

```
distance 95 165
```

distance (IPv6 Mobile)

To define an administrative distance for network mobility (NEMO) routes, use the **distance** command in router configuration mode. To return the administrative distance to its default distance definition, use the **no** form of this command.

distance [*mobile-distance*]

no distance

Syntax Description

mobile-distance	(Optional) Defines the mobile route, which is the default route for IPv6 over the roaming interface. The mobile default distance is 3.

Command Default

If no distances are configured, the default distances are automatically used.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The Mobile IPv6 NEMO router maintains the following type of route:

- Mobile route—Default route for IPv6 over the roaming interface

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Examples

The following example defines the administrative distance for the mobile route as 10:

```
Router(config-router)# distance 10
```

RelatedCommands

Command	Description
ipv6 router nemo	Enables the NEMO routing process on the home agent and places the router in router configuration mode.

distance (OSPFv3)

To configure an administrative distance for Open Shortest Path First version 3 (OSPFv3) routes inserted into the routing table, use the **distance** command in IPv6 or IPv4 address family configuration mode. To return the administrative distance to its default setting, use the **no** form of this command.

distance *distance*

no distance *distance*

Syntax Description

distance	The administrative distance. An integer from 10 to 254. (The values 0 to 9 are reserved for internal use. Routes with a distance value of 255 are not installed in the routing table.)

Command Default

Administrative distance is 110.

Command Modes

IPv6 address family configuration (config-router-af)
IPv4 address family configuration (config-router-af)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

If two processes attempt to insert the same route into the same routing table, the one with the lower administrative distance takes precedence.

An administrative distance is an integer from 10 to 254. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Examples

The following example configures an administrative distance of 200 for OSPFv3 in an IPv6 address family:

```
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# distance 200
```

RelateCommands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

distance bgp (IPv6)

To allow the use of external, internal, and local administrative distances that could be a better route than other external, internal, or local routes to a node, use the **distance bgp** command in address family configuration mode. To return to the default values, use the **no** form of this command

distance bgp *external-distance internal-distance local-distance*

no distance bgp

Syntax Description

external-distance	Administrative distance for Border Gateway Protocol (BGP) external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.
internal-distance	Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.
local-distance	Administrative distance for BGP local routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

Command Default

external-distance: 20
internal-distance: 200
local-distance: 200

Command Modes

Address family configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **distance bgp** (IPv6) command is similar to the **distance bgp** command, except that it is IPv6-specific. Settings configured by the **distance bgp** (IPv6) command will override the default IPv6 distance settings. IPv6 BGP is not influenced by the distance settings configured in IPv4 BGP router mode.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Distance values are subjective; there is no quantitative method for choosing the values.

Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

For IPv6 multicast BGP (MBGP) distance, the distance assigned is used in reverse path forwarding (RPF) lookup. Use the **show ipv6 rpf** command to display the distance assigned.

⚠ **Caution** Changing the administrative distance of BGP internal routes is considered dangerous to the system and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.

Examples

In the following address family configuration mode example, internal routes are known to be preferable to those learned through Interior Gateway Protocol (IGP), so the IPv6 BGP administrative distance values are set accordingly:

```
router bgp 65001
 neighbor 2001:0DB8::1 remote-as 65002
 address-family ipv6
 distance bgp 20 20 200
 neighbor 2001:0DB8::1 activate
 exit-address-family
```

Related Commands

Command	Description
show ipv6 rpf	Displays RPF information for a given unicast host address and prefix.

distribute-list prefix-list (IPv6 EIGRP)

To apply a prefix list to Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name*

no distribute-list prefix-list *list-name*

Syntax Description

list-name	Name of a prefix list. The list defines which EIGRP for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.

Command Default

Prefix lists are not applied to EIGRP for IPv6 routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The prefix list is applied to routing updates received or sent on all interfaces.

Examples

The following example applies prefix list list1 to routes received and sent on all interfaces:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# distribute-list prefix-list list1
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (IPv6 OSPF)

To apply a prefix list to Open Shortest Path First (OSPF) for IPv6 routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}

no distribute-list prefix-list *list-name* {**in** [*interface-type interface-number*] | **out** *routing-process* [*as-number*]}

Syntax Description

list-name	Name of a prefix list. The list defines which OSPF for IPv6 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.
out	Restricts which prefixes OSPF for IPv6 will identify to the other protocol.
routing-process	Name of a specific routing process. Valid entries for this value are **bgp, connected, eigrp**, **isis, ospf, rip,** or **static**.
as-number	(Optional) Autonomous system number, required for use with Border Gateway Protocol (BGP) and Routing Information Protocol (RIP).

Command Default

Prefix lists are not applied to OSPF for IPv6 routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Service Routers.
12.2(33) SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was modified. The **eigrp** and **ospf** keywords were added for the *routing process* argument.
15.1(2)T	This command was modified. The **eigrp** and **ospf** keywords were added for the *routing process* argument.

Usage Guidelines

If no interface is specified when the **in** keyword is used, the prefix list is applied to routing updates received on all interfaces.

Examples

The following example applies prefix list PL1 to routes received on Ethernet interface 0/0, and applies prefix list PL2 to advertised routes that came from process bgp 65:

```
Router(config)# ipv6 router ospf 1
Router(config-router)# distribute-list prefix-list PL1 in Ethernet0/0
Router(config-router)# distribute-list prefix-list PL2 out bgp 65
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

distribute-list prefix-list (IPv6 RIP)

To apply a prefix list to IPv6 Routing Information Protocol (RIP) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in router configuration mode. To remove the prefix list, use the **no** form of this command.

distribute-list prefix-list *listname* {**in** | **out**} [*interface-type interface-number*]

no distribute-list prefix-list *listname*

Syntax Description

listname	Name of a prefix list. The list defines which IPv6 RIP networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
out	Applies the prefix list to outgoing routing updates on the specified interface.
interface-type	(Optional) The specified interface type. For supported interface types, use the question mark (?) online help function.
interface-number	(Optional) The specified interface number.

Command Default

Prefix lists are not applied to IPv6 RIP routing updates.

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

If no interface is specified, the prefix list is applied to all interfaces.

Examples

The following example applies the prefix list named cisco to IPv6 RIP routing updates that are received on Ethernet interface 0/0:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr-rip)# distribute-list prefix-list cisco in ethernet 0/0
```

Related Commands

Command	Description
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

dns-server (IPv6)

To specify the Domain Name System (DNS) IPv6 servers available to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **dns-server** command in DHCP for IPv6 pool configuration mode. To remove the DNS server list, use the **no** form of this command.

dns-server *ipv6-address*

no dns-server *ipv6-address*

Syntax Description

ipv6-address	The IPv6 address of a DNS server. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

When a DHCP for IPv6 pool is first created, no DNS IPv6 servers are configured.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Multiple Domain Name System (DNS) server addresses can be configured by issuing this command multiple times. New addresses will not overwrite old addresses.

Examples

The following example specifies the DNS IPv6 servers available:

```
dns-server 2001:0DB8:3000:3000::42
```

Related Commands

Command	Description
domain-name	Configures a domain name for a DHCP for IPv6 client.
ipv6 dhcp pool	Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode.

domain-name (IPv6)

To configure a domain name for a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client, use the **domain-name** command in DHCPv6 pool configuration mode. To return to the default for this command, use the **no** form of this command.

domain-name *domain-name*

no domain-name

Syntax Description

domain-name	Default domain name used to complete unqualified hostnames. **Note** Do not include the initial period that separates an unqualified name from the domain name.

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCPv6 pool configuration mode (config-dhcp)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Use the **domain-name** command in IPv6 configure a domain name for a DHCPv6 client.

Examples

The following example configures a domain name for a DHCPv6 client:

```
Router(config)# ipv6 dhcp pool pool1
Router(cfg-dns-view)# domain-name domainv6
```

drop-unsecure

To drop messages with no or invalid options or an invalid signature, use the **drop-unsecure** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

drop-unsecure

no drop-unsecure

Syntax Description

This command has no arguments or keywords.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **drop-unsecure** command drops messages with no or invalid Cryptographically Generated Address (CGA) options or Rivest, Shamir, and Adelman (RSA) signature as per RFC 3971, *Secure Discovery (SeND)*. However, note that messages with an RSA signature or CGA options that do not conform with or are not verified per RFC 3972, *Cryptographically Generated Addresses (CGA)*, are dropped.

Use the **drop-unsecure** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and enables the router to drop messages with invalid CGA options or an invalid RSA signature:

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

dspfarm profile

To enter DSP farm profile configuration mode and define a profile for digital signal processor (DSP) farm services, use the **dspfarm profile** command in global configuration mode. To delete a disabled profile, use the **no** form of this command.

Cisco Unified Border Element

dspfarm profile *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]

no dspfarm profile *profile-identifier*

Cisco Unified Border Element (Enterprise) Cisco ASR 1000 Series Router

dspfarm profile *profile-identifier* {**transcode**}

no dspfarm profile *profile-identifier*

Cisco Integrated Services Routers Generation 2 (Cisco ISR G2)

dspfarm profile *profile-identifier* {**conference** [**video** [**homogeneous** | **heterogeneous** | **guaranteed-audio**]] | **mtp** | **transcode** [**video** | **universal**] } [**security**]

no dspfarm profile *profile-identifier*

Syntax Description

profile-identifier	Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.
conference	Enables a profile for conferencing.
mtp	Enables a profile for Media Termination Point (MTP).
transcode	Enables a profile for transcoding.
security	Enables a profile for secure DSP farm services.
video	(Optional) Enables a profile for video conferencing or transcoding.
homogeneous	(Optional) Specifies that all video participants use the one video format that is configured in this profile. DSP resources are reserved to support the conference at configuration time. **Note** The homogeneous profiles only support one video codec.
heterogeneous	(Optional) Specifies that video participants can use the different video formats that are configured in the profile. You can configure up to 10 video codecs in the heterogeneous profile. DSP resources are reserved to support the different configurations at configuration time.
guaranteed-audio	(Optional) Specifies that video participants in a heterogeneous conference will at least have an audio connection. You can configure up to 10 video codecs in the guaranteed-audio profile. The DSP resources for audio streams are reserved at configuration time, but DSP resources to support video conferences are not reserved. If the video endpoint supports the video format specified in the profile and DSP resources are available when the participant joins the conference, the participant joins as a video conferee in the video conference.

Command Default

If this command is not entered, no profiles are defined for the DSP farm services.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)XW	The **security** keyword was added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support for IPv6 was added.
15.0(1)M2 15.1(1)T	Support was modified for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 224 platforms.
Cisco IOS XE Release 3.2S	This command was modified. Support was added to the Cisco ASR 1000 Series Router. The **conference**, **mtp** and **security** keywords are not supported on the Cisco ASR 1000 Series Router in this release.
15.1(4)M	This command was modified. The **video** keyword was added.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to create a new profile or delete a disabled profile. After you create a new profile in dspfarm profile configuration mode, use the **no shutdown** command to enable the profile configuration, allocate resources and associate the profile with the application(s). If the profile cannot be enabled due to lack of resources, the system prompts you with a message "Can not enable the profile due to insufficient resources, resources available to support X sessions; please modify the configuration and retry."

If the DSP farm profile is successfully created, you enter the DSP farm profile configuration mode. You can configure multiple profiles for the same service.

Use the **no dspfarm profile** command to delete a profile from the system. If the profile is active, you cannot delete it; you must first disable it using the **shutdown** command. To modify a DSP farm profile, use the **shutdown** command in dspfarm profile configuration mode before you begin configuration.

The *profile identifier* uniquely identifies a profile. If the service type and *profile identifier* are not unique, the user is prompted with a message to choose a different profile identifier.

You must use the **security** keyword in order to enable secure DSP farm services such as secure transcoding.

Effective with Cisco IOS Releases 15.0(1)M2 and 15.1(1)T, platform support for the Cisco IAD 2430, IAD 2431, IAD 2432, and IAD 2435, and the Cisco VG 202, VG 204, and VG 225 is modified. These platforms are designed as TDM-IP devices and are not expandable to install extra DSP resources. So even though the **conference** keyword appears in the command syntax, this DSP service is not configurable on these platforms. If you try to configure conferencing on these platforms, the command-line interface displays the following message: "`%This platform does not support Conferencing feature.`"

The **transcode** keyword also appears in the command syntax, but this DSP service is not available on the Cisco VG 202, VG 204, and VG 224 platforms. If you try to configure transcoding on these platforms, the CLI displays the following message: “`%This platform does not support Transcoding feature.`”

Cisco ASR 1000 Series Router

The support for dspfarm profile command was added on Cisco ASR 1000 Series Router from Cisco IOS XE Release 3.2 and later releases. The command is used to create a dspfarm profile for different services.

Note The secure DSP farm services is always enabled for SPA-DSP on Cisco ASR 1000 Series Router. Only **transcode** keyword is supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s. The **conference**, **media**, and **security** keywords are not supported on Cisco ASR 1000 Series Router for Cisco IOS XE Release 3.2s.

In order to configure a video dspfarm profile, you must set **voice-service dsp-reservation** command to be less than 100 percent.

To enable dspfarm profiles for voice services, you must use the **dsp services dspfarm** command under the voice-card submode.

Examples

The following example enables DSP farm services profile 20 for conferencing:

```
Router(config)# dspfarm profile 20 conference
```

Note the response if the profile is already being used:

```
Router(config)# dspfarm profile 6 conference

Profile id 6 is being used for service TRANSCODING
 please select a different profile id
```

The following example enables DSP farm services profile 1 for transcoding:

```
Router(config)# dspfarm profile 1 transcode
```

Video Conferences

The following example enables DSP farm services profile 99 for homogeneous video. The conference supports four participants under one format (Video codec H.263, qcif resolution, and a frame-rate of 15 f/s).

```
Router(config)# dspfarm profile 99 conference video homogeneous
Router(config-dspfarm-profile)# codec h263 qcif frame-rate 15
Router(config-dspfarm-profile)# maximum conference-participant 4
```

Related Commands

Command	Description
dsp service dspfarm	Configures the DSP farm services for a specified voice card.
shutdown (DSP farm profile)	Disables the DSP farm profile.
voice-card	Enters voice card configuration mode
voice-service dsp-reservation	Configures the percentage of DSP resources are reserved for voice services and enables video services to use the remaining DSP resources.

eigrp event-log-size

To set the size of the Enhanced Interior Gateway Routing Protocol (EIGRP) event log, use the **eigrp event-log-size** command in router configuration mode or address-family topology configuration mode. To reset the size of the EIGRP event log to its default value, use the **no** form of this command.

eigrp event-log-size *size*

no eigrp event-log-size

Syntax Description

size	Size of the EIGRP event log; valid values are from 0 to half of the available memory on the system at the time of configuration. Default value is 500.

Command Default

The EIGRP event log size is 500.

Command Modes

Router configuration (config-router)
Address-family topology configuration (config-router-af-topology)

Command History

Release	Modification
12.2(18)SXF	This command was introduced in Cisco IOS Release 12.2(18)SXF.
15.0(1)M	This command was modified. Address-family topology configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When the configured size (number of lines) of the event log is exceeded, the last configured number of lines is retained, and the log becomes a rolling number of events with the most recent at the top of the log.

Examples

The following example shows how to set the size of the EIGRP event log to 5000010:

```
Router# configure terminal
Router(config)# router eigrp 2
Router (config-router)# eigrp event-log-size 5000010
Router (config-router)#
```

The following example shows how to set the size of the EIGRP event log in an EIGRP named configuration to 10000:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# topology base
Router(config-router-af-topology)# eigrp event-log-size 10000
```

Related Commands

Command	Description
clear ip eigrp event	Clears the IP EIGRP event log.

eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the **eigrp log-neighbor-changes** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of changes in EIGRP neighbor adjacencies, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Adjacency changes are logged.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)
Service-family configuration (config-router-sf)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the **no** form of this command.

To enable the logging of changes for EIGRP address-family neighbor adjacencies, use the **eigrp log-neighbor-changes** command in address-family configuration mode.

To enable the logging of changes for EIGRP service-family neighbor adjacencies, use the **eigrp log-neighbor-changes** command in service-family configuration mode.

Examples

The following configuration disables logging of neighbor changes for EIGRP process 209:

```
Router(config)# router eigrp 209
Router(config-router)# no eigrp log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 209:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp log-neighbor-changes
```

The following example shows how to disable logging of neighbor changes for EIGRP address-family with autonomous-system 4453:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# no eigrp log-neighbor-changes
Router(config-router-af)# exit-address-family
```

The following configuration enables logging of neighbor changes for EIGRP service-family process 209:

```
Router(config)# router eigrp 209
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp log-neighbor-changes
Router(config-router-sf)# exit-service-family
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp log-neighbor-warnings

To enable the logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of EIGRP neighbor warning messages, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. The range is from 1 to 65535. The default is 10.

Command Default

Neighbor warning messages are logged at 10-second intervals.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)
Service-family configuration (config-router-sf)

Command History

Release	Modification
12.0(5)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family and service-family configuration modes were added.
12.2(33)SRE	This command was modified. Address-family and service-family configuration modes were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

When neighbor warning messages occur, they are logged by default. With this command, you can disable and enable neighbor warning messages, and you can configure the interval between repeated neighbor warning messages.

To enable the logging of warning messages for an EIGRP address family, use the **eigrp log-neighbor-warnings** command in address-family configuration mode.

To enable the logging of warning messages for an EIGRP service family, use the **eigrp log-neighbor-warnings** command in service-family configuration mode.

Examples

The following command will log neighbor warning messages for EIGRP process 209 and repeat the warning messages in 5-minute (300 seconds) intervals:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the service family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Router(config)# router eigrp virtual-name
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp log-neighbor-warnings 300
```

The following example logs neighbor warning messages for the address family with autonomous system number 4453 and repeats the warning messages in five-minute (300 second) intervals:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
exit-address-family	Exits address-family configuration mode.
exit-service-family	Exits service-family configuration mode.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp router-id

To set the router ID used by Enhanced Interior Gateway Routing Protocol (EIGRP) when communicating with its neighbors, use the **eigrp router-id** command in router configuration mode, address-family configuration mode, or service-family configuration mode. To remove the configured router ID, use the **no** form of this command.

eigrp router-id *router-id*

no eigrp router-id [*router-id*]

Syntax Description

router-id	EIGRP router ID in IP address format.

Command Default

EIGRP automatically selects an IP address to use as the router ID when an EIGRP process is started. The highest local IP address is selected and loopback interfaces are preferred. The router ID is not changed unless the EIGRP process is removed with the **no router eigrp** command or if the router ID is manually configured with the **eigrp router-id** command.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)
Service-family configuration (config-router-sf)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)SRE	This command was modified. Address-family configuration mode and service-family configuration mode were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. The router ID can be configured with any IP address with two exceptions; 0.0.0.0 and 255.255.255.255 are not legal values and cannot be entered. A unique value should be configured for each router.

In EIGRP named IPv4, named IPv6, and Cisco Service Advertisement Framework (SAF) configurations, the *router-id* is also included for identifying internal routes and loop detection.

Examples

The following example configures 172.16.1.3 as a fixed router ID:

```
Router(config)# router eigrp 209
Router(config-router)# eigrp router-id 172.16.1.3
```

The following example configures 172.16.1.3 as a fixed router ID for service-family autonomous-system 4533:

```
Router(config)# router eigrp 209
Router(config-router)# service-family ipv4 autonomous-system 4453
Router(config-router-sf)# eigrp router-id 172.16.1.3
```

The following example configures 172.16.1.3 as a fixed router ID for address-family autonomous-system 4533:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
router eigrp	Configures the EIGRP routing process.
service-family	Specifies service-family configuration mode.

eigrp stub

To configure a router as a stub using Enhanced Interior Gateway Routing Protocol (EIGRP), use the **eigrp stub** command in router configuration mode or address-family configuration mode. To disable the EIGRP stub routing feature, use the **no** form of this command.

eigrp stub [**receive-only**] [**leak-map** *name*] [**connected**] [**static**] [**summary**] [**redistributed**]

no eigrp stub

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
leak-map *name*	(Optional) Allows dynamic prefixes based on a leak map.
connected	(Optional) Advertises connected routes.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Command Default

Stub routing is not enabled by default.

Command Modes

Router configuration (config-router)
Address-family configuration (config-router-af)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.
12.2	The **redistributed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified. Address-family configuration mode was added to support EIGRP named configurations. The **leak-map** keyword and *name* argument were added. This command replaces the **stub** command.
12.2(33)SRE	This command was modified. Address-family configuration mode was added to support EIGRP named configurations. The **leak-map** keyword and *name* argument were added. This command replaces the **stub** command.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.

Release	Modification
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)SXI4	This command was modified. Address-family configuration mode was added to support EIGRP named configurations. The **leak-map** keyword and *name* argument were added. This command replaces the **stub** command.

Usage Guidelines

Use the **eigrp stub** command to configure a router as a stub where the router directs all IP traffic to a distribution router, unless stub leaking is configured.

The **eigrp stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The four other optional keywords (**connected**, **static**, **summary**, **leak-map**, and **redistributed**) can be used in any combination but cannot be used with the **receive-only** keyword.

If any of these five keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword(s) will be sent. Route types specified by the remaining keywords will not be sent.

The **connected** keyword permits the EIGRP stub routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword permits the EIGRP stub routing feature to send static routes. Without the configuration of this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. It will still be necessary to redistribute static routes with the **redistribute static** command.

The **summary** keyword permits the EIGRP stub routing feature to send summary routes. Summary routes can be created manually with the **summary address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

The **redistributed** keyword permits the EIGRP stub routing feature to send other routing protocols and autonomous systems. Without the configuration of this option, EIGRP will not advertise redistributed routes.

The **leak-map** keyword permits the EIGRP stub routing feature to reference a leak map that identifies routes that are allowed to be advertised on an EIGRP stub router that would normally have been suppressed.

Examples

In the following example, the **eigrp stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub
```

In the following named configuration example, the **eigrp stub** command is used to configure the router as a stub that advertises routes learned from a directly connected client:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub connected
```

In the following example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# eigrp stub connected static
```

In the following named configuration example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub connected static
```

In the following example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0 eigrp
Router(config-router)# eigrp stub receive-only
```

In the following named configuration example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the router as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# eigrp stub receive-only
```

In the following example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the router to advertise other protocols and autonomous systems:

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0 eigrp
Router(config-router)# eigrp stub redistributed
```

In the following named configuration example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the router to advertise other protocols and autonomous systems:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af) eigrp stub redistributed
```

In the following example, the **eigrp stub** command is issued with the **leak-map** *name* keyword/argument pair to configure the router to reference a leak map that identifies routes that would normally have been suppressed:

```
Router(config)# router eigrp
Router(config-router)# network 10.0.0.0
Router(config-router) eigrp stub leak-map map1
```

In the following named configuration example, the **eigrp stub** command is issued with the **leak-map** *name* keyword/argument pair to configure the router to reference a leak map that identifies routes that would normally have been suppressed:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af) eigrp stub leak-map map1
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address-family process.

encapsulation

To set the encapsulation method used by the interface, use the **encapsulation** command in interface configuration mode. To remove the encapsulation, use the **no** form of this command.

encapsulation *encapsulation-type*

no encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type; one of the following keywords: • **atm-dxi**—ATM Mode-Data Exchange Interface. • **bstun**—Block Serial Tunnel. • **dot1q** *vlan-id* [**native**]—Enables IEEE 802.1q encapsulation of traffic on a specified subinterface in VLANs. The *vlan-id* argument is a virtual LAN identifier. The valid range is from 1 to 1000. The optional **native** keyword sets the PVID value of the port to the *vlan-id* value. • **frame-relay**—Frame Relay (for serial interface). • **hdlc**—High-Level Data Link Control (HDLC) protocol for serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces. • **isl** *vlan-id*—Inter-Switch Link (ISL) (for VLANs). • **lapb**—X.25 Link Access Procedure, Balanced. Data link layer protocol (LAPB) DTE operation (for serial interface). • **ppp**—PPP (for serial interface). • **sde** *said*—IEEE 802.10. The *said* argument is a security association identifier. This value is used as the VLAN identifier. The valid range is from 0 to 0xFFFFFFFE. • **sdlc**—IBM serial Systems Network Architecture (SNA). • **sdlc-primary**—IBM serial SNA (for primary serial interface). • **sdlc-secondary**—IBM serial SNA (for secondary serial interface). • **slip**—Specifies Serial Line Internet Protocol (SLIP) encapsulation for an interface configured for dedicated asynchronous mode or dial-on-demand routing (DDR). This is the default for asynchronous interfaces. • **smds**—Switched Multimegabit Data Services (SMDS) (for serial interface). • **ss7**—Sets the encapsulation type to SS7 and overrides the serial interface objects high-level data link control (HDLC) default.

Defaults

The default depends on the type of interface. For example, synchronous serial interfaces default to HDLC and asynchronous interfaces default to SLIP.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **sde** keyword was added to support IEEE 802.10
11.1	The **isl** keyword was added to support the Interswitch Link (ISL) Cisco protocol for interconnecting multiple switches and routers, and for defining virtual LAN (VLAN) topologies.
11.3(4)T	The **tr-isl trbrf-vla**n keyword was added to support TRISL, a Cisco proprietary protocol for interconnecting multiple routers and switches and maintaining VLAN information as traffic goes between switches.
12.0(1)T	The **dot1q** keyword was added to support IEEE 8021q standard for encapsulation of traffic on a specified subinterface in VLANs.
12.1(3)T	The **native** keyword was added.
12.2(11)T	This command was modified to include the **ss7** keyword in support of integrated signaling link terminal capabilities.
12.2(13)T	Support for IPv6 was added.
12.3(2)T	The **tr-isl trbrf-vla**n keyword was removed because support for the TRISL protocol is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

SLIP and PPP

To use SLIP or PPP, the router or access server must be configured with an IP routing protocol or with the **ip host-routing** command. This configuration is done automatically if you are using old-style **slip address** commands. However, you must configure it manually if you configure SLIP or PPP via the **interface async** command.

On lines configured for interactive use, encapsulation is selected by the user when they establish a connection with the **slip** or **ppp** EXEC command.

IP Control Protocol (IPCP) is the part of PPP that brings up and configures IP links. After devices at both ends of a connection communicate and bring up PPP, they bring up the control protocol for each network protocol that they intend to run over the PPP link such as IP or IPX. If you have problems passing IP packets and the **show interface** command shows that line is up, use the **negotiations** command to see if and where the negotiations are failing. You might have different versions of software running, or different versions of PPP, in which case you might need to upgrade your software or turn off PPP option negotiations. All IPCP options as listed in RFC 1332, *PPP Internet Protocol Control Protocol (IPCP)*, are supported on asynchronous lines. Only Option 2, TCP/IP header compression, is supported on synchronous interfaces.

PPP echo requests are used as keepalive packets to detect line failure. The **no keepalive** command can be used to disable echo requests. For more information about the **no keepalive** command, refer to the chapter “IP Services Commands” in the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services* and to the chapter “Configuring IP Services” in the *Cisco IOS IP Configuration Guide*.

To use SLIP or PPP, the Cisco IOS software must be configured with an IP routing protocol or with the **ip host-routing** command. This configuration is done automatically if you are using old-style **slip address** commands. However, you must configure it manually if you configure SLIP or PPP via the **interface async** command.

Note Disable software flow control on SLIP and PPP lines before using the **encapsulation** command.

SS7

The SS7 encapsulation command is new with the Integrated SLT feature and is available only for interface serial objects created by the **channel-group** command. For network access server (NAS) platforms, the encapsulation for channel group serial interface objects defaults to HDLC. You must explicitly set the encapsulation type to SS7 to override this default.

When encapsulation is set to SS7, the encapsulation command for that object is no longer available. A serial SS7 link is deleted only when its associated dial feature card (DFC) card is removed. As with existing Cisco 26*xx*-based SLTs, you do not need to specify whether the SS7 link is to be used as an A-link or an F-link.

By itself this command does not select the correct encapsulation type. Therefore, once created, you must set the encapsulation type to the new SS7 value, as well as assign a session channel ID to the link at the serial interface command level. The configuration on a digital SS7 link can be saved (**no shutdow**n) only when its encapsulation is successfully set to SS7 and it has been assigned a channel identifier.

VLANs

Do not configure encapsulation on the native VLAN of an IEEE 802.1q trunk without the **native** keyword. (Always use the **native** keyword when the *vlan-id* is the ID of the IEEE 802.1q native VLAN.)

For detailed information on use of this command with VLANs, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.

Examples

The following example shows how to reset HDLC serial encapsulation on serial interface 1:

```
Router(config)# interface serial 1
Router(config-if)# encapsulation hdlc
```

The following example shows how to enable PPP encapsulation on serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

The following example shows how to configure async interface 1 for PPP encapsulation:

```
Router(config)# interface async 1
Router(config-if)# encapsulation ppp
```

To learn more about the virtual serial interface and check SS7 encapsulation, enter the **show interfaces serial** *slot***/***trunk***:***channel-group* command in privileged EXEC mode, as in the following example:

```
Router# show interfaces serial 7/3:1

Serial7/3:1 is up, line protocol is down
 Hardware is PowerQUICC Serial
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 4/255, rxload 1/255
 Encapsulation SS7 MTP2, loopback not set
 Keepalive set (10 sec)
 Last input never, output 00:00:00, output hang never
 Last clearing of "show interface" counters 03:53:40
 Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 26000 bits/sec, 836 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  11580159 packets output, 46320636 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 output buffer failures, 0 output buffers swapped out
  2 carrier transitions
  DCD=up DSR=down DTR=down RTS=down CTS=down
```

Related Commands

Command	Description
channel-group	Assigns a channel group and selects the DSO time slots desired for SS7 links.
encapsulation x25	Specifies operation of a serial interface as an X.25 device.
keepalive	Sets the keepalive timer for a specific interface.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
ppp bap call	Sets PPP BACP call parameters.
slip	Starts a serial connection to a remote host using SLIP.

encapsulation frame-relay mfr

To create a multilink Frame Relay bundle link and to associate the link with a bundle, use the **encapsulation frame-relay mfr** command in interface configuration mode. To remove the bundle link from the bundle, use the **no** form of this command.

encapsulation frame-relay mfr *number* [*name*]

no encapsulation frame-relay mfr *number* [*name*]

Syntax Description

number	Interface number of the multilink Frame Relay bundle with which this bundle link will be associated.
name	(Optional) Bundle link identification (LID) name. The name can be up to 49 characters long. The default is the name of the physical interface.

Command Default

Frame Relay encapsulation is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced on the Cisco 12000 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

Use the *name* argument to assign a LID name to a bundle link. This name will be used to identify the bundle link to peer devices and to enable the devices to determine which bundle links are associated with which bundles. The LID name can also be assigned or changed by using the **frame-relay multilink lid** command on the bundle link interface. If the LID name is not assigned, the default name is the name of the physical interface.

Tips To minimize latency that results from the arrival order of packets, we recommend bundling physical links of the same line speed in one bundle.

To remove a bundle link from a bundle, use the **no encapsulation frame-relay mfr** command or configure a new type of encapsulation on the interface by using the **encapsulation** command.

Examples

The following example shows serial interface 0 being associated as a bundle link with bundle interface “mfr0.” The bundle link identification name is “BL1.”

```
interface mfr0
!
interface serial 0
 encapsulation frame-relay mfr0 BL1
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation	Sets the encapsulation method used by the interface.
frame-relay multilink lid	Assigns a LID name to a multilink Frame Relay bundle link.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

encryption {**des** | **3des** | **aes** | **aes 192** | **aes 256**}

no encryption

Syntax Description

des	56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	168-bit DES (3DES) as the encryption algorithm.
aes	128-bit Advanced Encryption Standard (AES) as the encryption algorithm.
aes 192	192-bit AES as the encryption algorithm.
aes 256	256-bit AES as the encryption algorithm.

Command History

The 56-bit DES-CBC encryption algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(2)T	The **3des** option was added.
12.2(13)T	The following keywords were added: **aes**, **aes 192**, and **aes 256**.
12.4(4)T	IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples

The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
 encryption 3des
 exit
```

The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured
    encryption method for ISAKMP policy 1
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

enrollment terminal (ca-trustpoint)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal [**pem**]

no enrollment terminal [**pem**]

Syntax Description

pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

No default behavior or values

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(4)T	The **pem** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

A user may want to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal.

The pem Keyword

Use the **pem** keyword to issue certificate requests (via the **crypto ca enroll** command) or receive issued certificates (via the **crypto ca import certificate** command) in PEM-formatted files through the console terminal. If the CA server does not support simple certificate enrollment protocol (SCEP), the certificate request can be presented to the CA server manually.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the **crypto ca authenticate** command.

Examples

The following example shows how to manually specify certificate enrollment via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
 enrollment terminal
 crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca enroll	Obtains the certificates of your router from the certification authority.
crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment url (ca-trustpoint)

To specify the enrollment parameters of a certification authority (CA), use the **enrollment url** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

no enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]

Syntax Description

mode	(Optional) Specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
retry period *minutes*	(Optional) Specifies the period in which the router will wait before sending the CA another certificate request. The default is 1 minute between retries. (Specify from 1 to 60 minutes.)
retry count *number*	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 to 100 retries.)
url *url*	Specifies the URL of the file system where your router should send certificate requests. For enrollment method options, see Table 27.
pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Defaults

Your router does not know the CA URL until you specify it using the **url** *url* keyword and argument.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3T	This command was introduced as the **enrollment url** (ca-identity) command.
12.2(8)T	This command replaced the **enrollment url** (ca-identity) command. The **mode**, **retry period** *minutes*, and **retry count** *number* keywords and arguments were added.
12.2(13)T	The **url** *url* option was enhanced to support TFTP enrollment.
12.3(4)T	The **pem** keyword was added, and the **url** *url* option was enhanced to support an additional enrollment method—the Cisco IOS File System (IFS).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified period of time (the retry period), the router will send another certificate request. By default, the router will send a maximum of ten requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified via the **retry count** *number* option) is exceeded.

Use the **pem** keyword to issue certificate requests (using the **crypto pki enroll** command) or receive issued certificates (using the **crypto pki import certificate** command) in PEM-formatted files.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained using the **crypto ca authenticate** command.

Use the **url** *url* option to specify or change the URL of the CA. Table 27 lists the available enrollment methods.

Table 27 Certificate Enrollment Methods

Enrollment Method	Description
bootflash	Enroll via bootflash: file system
cns	Enroll via Cisco Networking Services (CNS): file system
flash	Enroll via flash: file system
ftp	Enroll via FTP: file system
null	Enroll via null: file system
nvram	Enroll via NVRAM: file system
rcp	Enroll via remote copy protocol (rcp): file system
scp	Enroll via secure copy protocol (scp): file system
SCEP[1]	Enroll via Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL)
system	Enroll via system: file system
TFTP[2]	Enroll via TFTP: file system

[1] If you are using SCEP for enrollment, the URL must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.

[2] If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file_specification is optional. See the section “TFTP Certificate Enrollment” for additional information.)

TFTP Certificate Enrollment

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router will append an extension onto the file specification. When the **crypto pki authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the FQDN of the router will be used.)

Note The **crypto pki trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related commands (all **ca-identity** and **trusted-root** configuration mode commands). If you enter a **ca-identity** or **trusted-root** command, the configuration mode and command will be written back as pki-trustpoint.

Examples

The following example shows how to declare a CA named “trustpoint” and specify the URL of the CA as “http://example:80”:

```
crypto pki trustpoint trustpoint
 enrollment url http://example:80
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.

eui-interface

To use the Media Access Control (MAC) address from a specified interface for deriving the IPv6 mobile home address, use the **eui-interface** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

eui-interface *interface-type interface-number*

no eui-interface *interface-type interface-number*

SyntaxDescription

interface-type interface-number	Interface type and number from which the MAC address is derived.

Command Default

A MAC address is not used to derive the IPv6 mobile home address.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the **eui-interface** command to physically connect to the MAC to get the EUI-64 interface ID.

Examples

In the following example, the router derives the EUI-64 interface ID from the specified interface:

```
eui-interface Ethernet 0/0
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

evaluate (IPv6)

To nest an IPv6 reflexive access list within an IPv6 access list, use the **evaluate** (IPv6) command in IPv6 access list configuration mode. To remove the nested IPv6 reflexive access list from the IPv6 access list, use the **no** form of this command.

evaluate *access-list-name* [**sequence** *value*]

no evaluate *access-list-name* [**sequence** *value*]

Syntax Description

access-list-name	The name of the IPv6 reflexive access list that you want evaluated for IPv6 traffic entering your internal network. This is the name defined in the **permit** (IPv6) command. Names cannot contain a space or quotation mark, or begin with a numeric.
sequence *value*	(Optional) Specifies the sequence number for the IPv6 reflexive access list. The acceptable range is from 1 to 4294967295.

Command Default

IPv6 reflexive access lists are not evaluated.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **evaluate** (IPv6) command is similar to the **evaluate** (IPv4) command, except that it is IPv6-specific.

This command is used to achieve IPv6 reflexive filtering, a form of session filtering.

Before this command will work, you must define the IPv6 reflexive access list using the **permit** (IPv6) command.

This command nests an IPv6 reflexive access list within an IPv6 access control list (ACL).

If you are configuring an IPv6 reflexive access list for an external interface, the IPv6 ACL should be one that is applied to inbound traffic. If you are configuring IPv6 reflexive access lists for an internal interface, the IPv6 ACL should be one that is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the IPv6 reflexive access list.)

This command allows IPv6 traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IPv6 ACL; the entry “points” to the IPv6 reflexive access list to be evaluated.

As with all IPv6 ACL entries, the order of entries is important. Normally, when a packet is evaluated against entries in an IPv6 ACL, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With an IPv6 reflexive access list nested in an IPv6 ACL, the IPv6 ACL entries are evaluated sequentially up to the nested entry, then the IPv6 reflexive access list entries are evaluated sequentially, and then the remaining entries in the IPv6 ACL are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

Note IPv6 reflexive access lists do not have any implicit deny or implicit permit statements.

Examples

The **evaluate** command in the following example nests the temporary IPv6 reflexive access lists named TCPTRAFFIC and UDPTRAFFIC in the IPv6 ACL named OUTBOUND. The two reflexive access lists are created dynamically (session filtering is “triggered”) when incoming TCP or UDP traffic matches the applicable permit entry in the IPv6 ACL named INBOUND. The OUTBOUND IPv6 ACL uses the temporary TCPTRAFFIC or UDPTRAFFIC access list to match (evaluate) outgoing TCP or UDP traffic related to the triggered session. The TCPTRAFFIC and UDPTRAFFIC lists time out automatically when no IPv6 packets match the permit statement that triggered the session (the creation of the temporary reflexive access list).

Note The order of IPv6 reflexive access list entries is not important because only permit statements are allowed in IPv6 reflexive access lists and reflexive access lists do not have any implicit conditions. The OUTBOUND IPv6 ACL simply evaluates the UDPTRAFFIC reflexive access list first and, if there were no matches, the TCPTRAFFIC reflexive access list second. Refer to the **permit** command for more information on configuring IPv6 reflexive access lists.

```
ipv6 access-list INBOUND
  permit tcp any any eq bgp reflect TCPTRAFFIC
  permit tcp any any eq telnet reflect TCPTRAFFIC
  permit udp any any reflect UDPTRAFFIC

ipv6 access-list OUTBOUND
  evaluate UDPTRAFFIC
  evaluate TCPTRAFFIC
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

event-log

To enable event logging for applications, use the **event-log** command in application configuration monitor configuration mode. To disable event logging, use the **no** form of this command.

event-log [**size** [*number of events*]] [**one-shot**] [**pause**]

no event-log

SyntaxDescription

size [*number of events*]	(Optional) Maximum number of OSPF events in the event log.
one-shot	(Optional) Mode that enables the logging of new events at one specific point in time. The event logging mode is cyclical by default, meaning that all new events are logged as they occur.
pause	(Optional) Enables the user to pause the logging of any new events at any time, while keeping the current events in the log.

Command Default

By default, event logging is not enabled.
When event logging is enabled, it is cyclical by default.

Command Modes

Application configuration monitor configuration mode
OSPF for IPv6 router configuration mode

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application event-log** command.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

This command enables event logging globally for all voice applications. To enable or disable event logging for a specific application, use one of the following commands:

param event-log (application parameter configuration mode)

paramspace appcommon event-log (service configuration mode)

Note To prevent event logging from adversely impacting system resources for production traffic, the gateway uses a throttling mechanism. When free processor memory drops below 20-percent, the gateway automatically disables all event logging. It resumes event logging when free memory rises above 30 percent. While throttling is occurring, the gateway does not capture any new event logs even if event logging is enabled. You should monitor free memory and enable event logging only when necessary for isolating faults.

Examples

The following example shows event logging enabled:

```
application
 monitor
  event-log
```

The following example shows OSPF for IPv6 event logging enabled. The router instance is 1, the event-log size is 10,000, and the mode is one-shot.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
```

Related Commands

Command	Description
call application event-log	Enables event logging for all voice application instances.
event-log dump ftp	Enables the gateway to write the contents of the application event log buffer to an external file.
event-log error-only	Restricts event logging to error events only for application instances.
event-log max-buffer-size	Sets the maximum size of the event log buffer for each application instance.
param event-log	Enables or disables event logging for a package.
paramspace appcommon event-log	Enables or disables event logging for a service (application).

event-log (OSPFv3)

To enable Open Shortest Path First version 3 (OSPFv3) event logging in an IPv4 OSPFv3 process, use the **event-log** command in OSPFv3 router configuration mode. To disable this feature, use the **no** version of the command.

event-log [**one-shot** | **pause** | **size** *number-of-events*]

Syntax Description

one-shot	(Optional) Disables OSPFv3 event logging when the log buffer becomes full.
pause	(Optional) Pauses the event logging function.
size *number-of-events*	(Optional) Configures the maximum number of events stored in the event log. The range is from 1 through 65534.

Command Default

Event logging is not enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

Examples

The following examples show how to enable event logging in an IPv4 OSPFv3 process:

```
Router(config)# router ospfv3 1
Router(config-router)# event-log
```

RelatedCommands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

explicit-prefix

To register IPv6 prefixes connected to the IPv6 mobile router, use the **explicit-prefix** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

explicit-prefix

no explicit-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No IPv6 prefixes are specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The mobile router presents a list of prefixes to the home agent as part of the binding update procedure. If the home agent determines that the mobile router is authorized to use these prefixes, it sends a bind acknowledgment message.

Examples

The following example shows how to register connected IPv6 prefixes:

```
Router(IPv6-mobile-router)# explicit-prefix
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

fabric switching-mode allow

To enable various switching modes in the presence of two or more fabric-enabled switching modules, use the **fabric switching-mode allow** command in global configuration mode. To disable the settings, use the **no** form of this command.

fabric switching-mode allow {**bus-mode** | **dcef-only** | **truncated** [**threshold** [*mod*]]}

no fabric switching-mode allow {**bus-mode** | **truncated** [**threshold**]}

Syntax Description

bus-mode	Specifies a module to run in bus mode.
dcef-only	Allows switching in distributed Cisco Express Forwarding (dCEF)-only mode.
truncated	Specifies a module to run in truncated mode.
threshold *mod*	(Optional) Specifies the number of fabric-enabled modules for truncated switching mode; see the "Usage Guidelines" section for additional information.

Command Default

The truncated mode is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command supports the Supervisor Engine 2.
12.2(18)SXD1	This command was modified. The **dcef-only** keyword was added on the Supervisor Engine 2.
12.2(18)SXE	This command was modified. Support for OIR performance enhancement and the **dcef-only** keyword was added on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was modified. This command was introduced on the Supervisor Engine 720-10GE.

Usage Guidelines

This command is not supported on Catalyst 6500 or Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Ethernet ports are not disabled when this command is entered on a Supervisor Engine 720-10GE. This command is also supported with Supervisor Engine 720 starting with Release 12.2(33)SXI2. However, prior to Release 12.2(33)SXI2, if all the installed switching modules have Distributed Forwarding Cards (DFCs), enter the **fabric switching-mode allow dcef-only** command to disable the Ethernet ports on both supervisor engines. Entering this command ensures that all modules are operating in dCEF-only mode and simplifies switchover to the redundant supervisor engine.

With a Supervisor Engine 2 and Release 12.2(18)SXD1 and later releases, if all the installed switching modules have DFCs, enter the **fabric switching-mode allow dcef-only** command to disable the Ethernet ports on the redundant supervisor engine. Entering this command ensures that all modules are operating in dCEF-only mode.

Note The **fabric switching-mode allow dcef-only** command is accepted only in stateful switchover (SSO) redundancy mode.

Bus mode—Supervisor engines use this mode for traffic between nonfabric-enabled modules and for traffic between a nonfabric-enabled module and a fabric-enabled module. In this mode, all traffic passes between the local bus and the supervisor engine bus.

dCEF-only—Supervisor engines, both active and redundant, operate as nonfabric-capable modules with their uplink ports relying on the Policy Feature Card (PFC) on the active supervisor engine for all forwarding decisions. For the Supervisor 720-10G, the uplink ports on both the active and standby routers will remain active. If all other modules are operating in dCEF-only mode, module Online Insertion and Removal (OIR) is nondisruptive.

Note The system message “PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL” is displayed on the Supervisor Engine if both the **fabric switching-mode allow dcef-only** and **ipv6 mfib hardware-switching uplink** commands are configured. The router will ignore the command configured last.

Truncated mode—Supervisor engines use this mode for traffic between fabric-enabled modules when there are both fabric-enabled and nonfabric-enabled modules installed. In this mode, line cards send a truncated version of the traffic (the first 64 bytes of the frame) over the Catalyst bus.

Compact mode—Supervisor engines use this mode for all traffic when only fabric-enabled modules are installed. In this mode, a compact version of the Desktop Bus (DBus) header is forwarded over the Catalyst bus, which provides the best possible centralized forwarding performance.

A fabric-enabled module has an additional connection directly to the switch fabric. Fabric-enabled modules forward packets in compressed mode, where only the header is sent to the Supervisor Engine and the full packet is forwarded directly from one line card to another.

To prevent use of nonfabric-enabled modules or to prevent fabric-enabled modules from using bus mode, enter the **no fabric switching-mode allow bus-mode** command.

Caution Entering the **no fabric switching-mode allow bus-mode** command removes power from any nonfabric-enabled modules that are installed.

The **fabric switching-mode allow** command affects Supervisor engines that are configured with a minimum of two fabric-enabled modules.

You can enter the **fabric switching-mode allow truncated** command to unconditionally allow truncated mode.

You can enter the **no fabric switching-mode allow truncated** command to allow truncated mode if the threshold is met.

You can enter the **no fabric switching-mode allow bus-mode** command to prevent any module from running in bus mode.

To return to the default truncated-mode threshold, enter the **no fabric switching-mode allow truncated threshold** command.

The valid value for *mod* is the threshold value.

Examples

The following example shows how to specify truncated mode:

```
Router(config)# fabric switching-mode allow truncated
```

Related Commands

Command	Description
ipv6 mfib hardware-switching uplink	Configures MFIB hardware switching for IPv6 multicast packets on a global basis.
show fabric	Displays the information about the crossbar fabric.

fingerprint

To preenter a fingerprint that can be matched against the fingerprint of a certification authority (CA) certificate during authentication, use the **fingerprint** command in ca-trustpoint configuration mode. To remove the preentered fingerprint, use the **no** form of this command.

fingerprint *ca-fingerprint*

no fingerprint *ca-fingerprint*

Syntax Description

ca-fingerprint	Certificate fingerprint.

Defaults

A fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(12)	This command was introduced. This release supports only message digest algorithm 5 (MD5) fingerprints.
12.3(13)T	Support was added for Secure Hash Algorithm 1 (SHA1), but only for Cisco IOS T releases.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Note An authentication request made using the CLI is considered an interactive request. An authentication request made using HTTP or another management tool is considered a noninteractive request.

Preenter the fingerprint if you want to avoid responding to the verify question during CA certificate authentication or if you will be requesting authentication noninteractively. The preentered fingerprint may be either the MD5 fingerprint or the SHA1 fingerprint of the CA certificate.

If you are authenticating a CA certificate and the fingerprint was preentered, if the fingerprint matches that of the certificate, the certificate is accepted. If the preentered fingerprint does not match, the certificate is rejected.

If you are requesting authentication noninteractively, the fingerprint must be preentered or the certificate will be rejected. The verify question will not be asked when authentication is requested noninteractively.

If you are requesting authentication interactively without preentering the fingerprint, the fingerprint of the certificate will be displayed, and you will be asked to verify it.

Examples

The following example shows how to preenter an MD5 fingerprint before authenticating a CA certificate:

```
Router(config)# crypto pki trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint) exit
Router(config)# crypto pki authenticate myTrustpoint
Certificate has the following attributes:
       Fingerprint MD5: 6513D537 7AEA61B7 29B7E8CD BBAA510B
      Fingerprint SHA1: 998CCFAA 5816ECDE 38FC217F 04C11F1D DA06667E
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router (config)#
```

The following is an example for Cisco Release 12.3(12). Note that the SHA1 fingerprint is not displayed because it is not supported by this release.

```
Router(config)# crypto ca trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint)# exit
Router(config)# crypto ca authenticate myTrustpoint
Certificate has the following attributes:
           Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca trustpoint	Declares the CA that your router should use.

frame-relay interface-dlci

To assign a data-link connection identifier (DLCI) to a specified Frame Relay subinterface on the router or access server, to assign a specific permanent virtual circuit (PVC) to a DLCI, or to apply a virtual template configuration for a PPP session, use the **frame-relay interface-dlci** command in interface configuration mode. To remove this assignment, use the **no** form of this command.

frame-relay interface-dlci *dlci* [**ietf** | **cisco**] [**voice-cir** *cir*] [**ppp** *virtual-template-name*]

no frame-relay interface-dlci *dlci* [**ietf** | **cisco**] [**voice-cir** *cir*] [**ppp** *virtual-template-name*]

BOOTP Server Only

frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

no frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

Syntax Description

dlci	DLCI number to be used on the specified subinterface.
ietf	(Optional) Specifies Internet Engineering Task Force (IETF) as the type of Frame Relay encapsulation.
cisco	(Optional) Specifies Cisco encapsulation as the type of Frame Relay encapsulation.
voice-cir *cir*	(Optional; supported on the Cisco MC3810 only.) Specifies the upper limit on the voice bandwidth that may be reserved for this DLCI. The default is the committed information rate (CIR) configured for the Frame Relay map class. For more information, see the "Usage Guidelines" section.
ppp	(Optional) Enables the circuit to use the PPP in Frame Relay encapsulation.
virtual-template-name	(Optional) Name of the virtual template interface to apply the PPP connection to.
protocol ip *ip-address*	(Optional) Indicates the IP address of the main interface of a new router or access server onto which a router configuration file is to be automatically installed over a Frame Relay network. Use this option only when this device will act as the BOOTP server for automatic installation over Frame Relay.

Command Default

No DLCI is assigned.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-subif)

Command History

Release	Modification
10.0	This command was introduced.
11.3(1)MA	The **voice-encap** option was added for the Cisco MC3810.
12.0(1)T	The **ppp** keyword and *virtual-template-name* argument were added.
12.0(2)T	The **voice-cir** option was added for the Cisco MC3810.
12.0(3)T	The **x25 profile** keyword was added.
12.0(4)T	Usage guidelines for the Cisco MC3810 were added.
12.0(7)XK	The **voice-encap** keyword for the Cisco MC3810 was removed. This keyword is no longer supported.
12.1(2)T	The **voice-encap** keyword for the Cisco MC3810 was removed. This keyword is no longer supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command is typically used for subinterfaces; however, it can also be used on main interfaces. Using the **frame-relay interface-dlci** command on main interfaces will enable the use of routing protocols on interfaces that use Inverse ARP. The **frame-relay interface-dlci** command on a main interface is also valuable for assigning a specific class to a single PVC where special characteristics are desired. Subinterfaces are logical interfaces associated with a physical interface. You must specify the interface and subinterface before you can use this command to assign any DLCIs and any encapsulation or broadcast options.

A DLCI cannot be configured on a subinterface if the same DLCI has already been configured on the main interface. If the same DLCI is to be configured on the subinterface as on the main interface, the DLCI on the main interface must be removed first before it is configured on the subinterface. The DLCI on the main interface can be removed by using the **no frame-relay interface-dlci** command on the main interface.

This command is required for all point-to-point subinterfaces; it is also required for multipoint subinterfaces for which dynamic address resolution is enabled. It is not required for multipoint subinterfaces configured with static address mappings.

Use the **protocol ip** *ip-address* option only when this router or access server will act as the BOOTP server for auto installation over Frame Relay.

By issuing the **frame-relay interface-dlci** interface configuration command, you enter Frame Relay DLCI interface configuration mode (see the first example below). This gives you the following command options, which must be used with the relevant class or X.25-profile names you previously assigned:

- **class** *name*—Assigns a map class to a DLCI.
- **default**—Sets a command to its defaults.
- **no** {**class** *name* | **x25-profile** *name*}—Cancels the relevant class or X.25 profile.
- **x25-profile** *name*—Assigns an X.25 profile to a DLCI. (Annex G.)

A Frame Relay DLCI configured for Annex G can be thought of as a single logical X.25/LAPB interface. Therefore, any number of X.25 routes may be configured to route X.25 calls to that logical interface.

The **voice-cir** option on the Cisco MC3810 provides call admission control; it does not provide traffic shaping. A call setup will be refused if the unallocated bandwidth available at the time of the request is not at least equal to the value of the **voice-cir** option.

When configuring the **voice-cir** option on the Cisco MC3810 for Voice over Frame Relay, do not set the value of this option to be higher than the physical link speed. If Frame Relay traffic shaping is enabled for a PVC that is sharing voice and data, do not configure the **voice-cir** option to be higher than the value set with the **frame-relay mincir** command.

Note On the Cisco MC3810 only, the **voice-cir** option performs the same function as the **frame-relay voice bandwidth** map-class configuration command introduced in Cisco IOS Release 12.0(3)XG.

Examples

The following example assigns DLCI 100 to serial subinterface 5.17:

```
! Enter interface configuration and begin assignments on interface serial 5.
interface serial 5
! Enter subinterface configuration by assigning subinterface 17.
interface serial 5.17
! Now assign a DLCI number to subinterface 5.17.
frame-relay interface-dlci 100
```

The following example specifies DLCI 26 over serial subinterface 1.1 and assigns the characteristics under virtual-template 2 to this PPP connection:

```
Router(config)# interface serial1.1 point-to-point
Router(config-if)# frame-relay interface-dlci 26 ppp virtual-template2
```

The following example shows an Annex G connection being created by assigning the X.25 profile “NetworkNodeA” to Frame Relay DLCI interface 20 on serial interface 1 (having enabled Frame Relay encapsulation on that interface):

```
Router(config)# interface serial 1
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay interface-dlci 20
Router(config-fr-dlci)# x25-profile NetworkNodeA
```

The following example assigns DLCI 100 to serial subinterface 5.17:

```
Router(config)# interface serial 5
Router(config-if)# interface serial 5.17
Router(config-if)# frame-relay interface-dlci 100
```

The following example assigns DLCI 80 to the main interface first and then removes it before assigning the same DLCI to the subinterface. The DLCI must be removed from the main interface first, because the same dlci cannot be assigned to the subinterface after already being assigned to the main interface:

```
Router(config)# interface serial 2/0
Router(config-if)# encapsulation frame-relay
Router(config-if)# frame-relay interface-dlci 80
Router(config-fr-dlci)# exit
Router(config-if)# interface serial 2/0
Router(config-if)# no frame-relay interface-dlci 80
Router(config-if)# interface serial 2/0.1
Router(config-subif)# frame-relay interface-dlci 80
```

Related Commands

Command	Description
frame-relay class	Associates a map class with an interface or subinterface.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interface	Displays P1024B/C information.
vofr	Configures subchannels and enables Voice over Frame Relay for a specific DLCI.

frame-relay intf-type

To configure a Frame Relay switch type, use the **frame-relay intf-type** command in interface configuration mode. To disable the switch, use the **no** form of this command.

frame-relay intf-type [**dce** | **dte** | **nni**]

no frame-relay intf-type [**dce** | **dte** | **nni**]

Syntax Description

dce	(Optional) Router or access server functions as a switch connected to a router.
dte	(Optional) Router or access server is connected to a Frame Relay network.
nni	(Optional) Router or access server functions as a switch connected to a switch—supports Network-to-Network Interface (NNI) connections.

Defaults

The router or access server is connected to a Frame Relay network.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command can be used only if Frame Relay switching has previously been enabled globally by means of the **frame-relay switching** command.

Examples

The following example configures a DTE switch type:

```
frame-relay switching
!
interface serial 2
 frame-relay intf-type dte
```

frame-relay map ipv6

To define the mapping between a destination IPv6 address and the data-link connection identifier (DLCI) used to connect to the destination address, use the **frame-relay map ipv6** command in interface configuration mode. To delete the map entry, use the **no** form of this command.

frame-relay map ipv6 *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]

no frame-relay map ipv6 *ipv6-address*

Syntax Description

ipv6-address	Destination IPv6 (protocol) address that is being mapped to a permanent virtual circuit (PVC). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dlci	DLCI number used to connect to the specified protocol address on the interface. The acceptable range is from 16 to 1007.
broadcast	(Optional) Forwards IPv6 multicast packets to this address when multicast is not enabled (see the **frame-relay multicast-dlci** command for more information about multicasts). **Note** IPv6 supports multicast packets; broadcast packets are not supported.
cisco	(Optional) Cisco encapsulation method.
ietf	(Optional) Internet Engineering Task Force (IETF) Frame Relay encapsulation method. Used when the router or access server is connected to the equipment of another vendor across a Frame Relay network.
payload-compression	(Optional) Enables payload compression.
packet-by-packet	(Optional) Packet-by-packet payload compression using the Stacker method.
frf9 stac	(Optional) FRF.9 compression using the Stacker method: • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the Versatile Interface Processor (VIP2) (distributed compression). • If the second-generation VIP2 is not available, compression is performed in the main processor of the router (software compression).

data-stream stac	(Optional) Data-stream compression using the Stacker method: • If the router contains a CSA, compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the main processor of the router (software compression).
hardware-options	(Optional) Choose one of the following hardware options: • **distributed**—Specifies that compression is implemented in the software that is installed in the VIP2. If the VIP2 is not available, compression is performed in the main processor of the router (software compression). This option applies only to the Cisco 7500 series routers. This option is not supported with data-stream compression. • **software**—Specifies that compression is implemented in the Cisco IOS software installed in the main processor of the router. • **csa** *csa-number*—Specifies the CSA to use for a particular interface. This option applies only to Cisco 7200 series routers.

Command Default

No mapping is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **frame-relay map ipv6** command is similar to the **frame-relay map** command, except that it is IPv6-specific.

Many DLCIs can be known by a router or access server and can send data to many different places, but they are all multiplexed over one physical link. The Frame Relay map defines the logical connection between a specific protocol and address pair and the correct DLCI.

The optional **ietf** and **cisco** keywords allow flexibility in the configuration. If no keywords are specified, the map inherits the attributes set with the **encapsulation frame-relay** command. You can also use the encapsulation options to specify that, for example, all interfaces use IETF encapsulation except one, which needs the original Cisco encapsulation method and can be configured through use of the **cisco** keyword with the **frame-relay map ipv6** command.

Data-stream compression is supported on interfaces and virtual circuits (VCs) using Cisco proprietary encapsulation. When the **data-stream stac** keywords are specified, Cisco encapsulation is automatically enabled. FRF.9 compression is supported on IETF-encapsulated VCs and interfaces. When the **frf9 stac** keywords are specified, IETF encapsulation is automatically enabled.

Packet-by-packet compression is Cisco-proprietary and will not interoperate with routers of other manufacturers.

You can disable payload compression by entering the **no frame-relay map ipv6 payload-compression** command and then entering the **frame-relay map ipv6** command again with one of the other encapsulation keywords (**ietf** or **cisco**).

Use the **frame-relay map ipv6** command to enable or disable payload compression on multipoint interfaces. Use the **frame-relay payload-compression** command to enable or disable payload compression on point-to-point interfaces.

We recommend that you shut down the interface before changing encapsulation types. Although not required, shutting down the interface ensures that the interface is reset for the new encapsulation.

Examples

In the following example, three nodes named Cisco A, Cisco B, and Cisco C make up a fully meshed network. Each node is configured with two PVCs, which provide an individual connection to each of the other two nodes. Each PVC is configured on a different point-to-point subinterface, which creates three unique IPv6 networks (2001:0DB8:2222:1017::/64, 2001:0DB8:2222:1018::/64, and 2001:0DB8:2222:1019::/64). Therefore, the mappings between the IPv6 addresses of each node and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses are implicit (no additional mappings are required).

Note Given that each PVC in the following example is configured on a different point-to-point subinterface, the configuration in the following example can also be used in a network that is not fully meshed. Additionally, configuring each PVC on a different point-to-point subinterface can help simplify your routing protocol configuration. However, the configuration in the following example requires more than one IPv6 network, whereas configuring each PVC on point-to-multipoint interfaces requires only one IPv6 network.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
!
interface Serial3.17 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1017::46/64
 frame-relay interface-dlci 17
!
interface Serial3.19 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1019::46/64
 frame-relay interface-dlci 19
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
!
interface Serial5.17 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1017::73/64
 frame-relay interface-dlci 17
!
interface Serial5.18 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1018::73/64
 frame-relay interface-dlci 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
!
interface Serial0.18 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1018::72/64
 frame-relay interface-dlci 18
!
interface Serial0.19 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1019::72/64
 frame-relay interface-dlci 19
```

In the following example, the same three nodes (Cisco A, Cisco B, and Cisco C) from the previous example make up a fully meshed network and each node is configured with two PVCs (which provide an individual connection to each of the other two nodes). However, the two PVCs on each node in the following example are configured on a single interface (serial 3, serial 5, and serial 10, respectively), which makes each interface a point-to-multipoint interface. Therefore, explicit mappings are required between the link-local and global IPv6 addresses of each interface on all three nodes and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::46/64
 frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::72 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 17
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::73/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 17
 frame-relay map ipv6 2001:0DB8:2222:1044::72 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::72/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast
```

```
frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast
frame-relay map ipv6 2001:0DB8:2222:1044::46 19
frame-relay map ipv6 2001:0DB8:2222:1044::73 18
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay payload-compress	Enables Stacker payload compression on a specified point-to-point interface or subinterface.

frame-relay multilink ack

To configure the number of seconds for which a bundle link will wait for a hello message acknowledgment before resending the hello message, use the **frame-relay multilink ack** command in interface configuration mode. To reset this parameter to the default setting, use the **no** form of this command.

frame-relay multilink ack *seconds*

no frame-relay multilink ack

Syntax Description

seconds	Number of seconds for which a bundle link will wait for a hello message acknowledgment before resending the hello message. Range: 1 to 10. Default: 4.

Command Default

The default acknowledgement interval is 4 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

The **frame-relay multilink ack** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Both ends of a bundle link send out hello messages at regular intervals. When a peer device receives a hello message, it responds by sending an acknowledgment. This exchange of hello messages and acknowledgments serves as a keepalive mechanism for the link. If the bundle link sends a hello message but does not receive an acknowledgment, it will resend the hello message up to a configured maximum number of times. If the bundle link exhausts the maximum number of retries, the bundle link line protocol is considered down (nonoperational).

The **frame-relay multilink ack** command setting on the local router is independent of the setting on the peer device.

Examples

The following example shows how to configure the bundle link to wait 6 seconds before resending hello messages:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink ack 6
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.
frame-relay multilink hello	Configures the interval at which a bundle link will send out hello messages.
frame-relay multilink retry	Configures the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment.

frame-relay multilink bid

To assign a bundle identification (BID) name to a multilink Frame Relay bundle, use the **frame-relay multilink bid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink bid *name*

no frame-relay multilink bid

Syntax Description

name	Bundle identification (BID) name. The name can be up to 49 characters long. The default is "mfr" followed by the number assigned to the bundle using the **interface mfr** command; for example, "mfr0."

Command Default

The BID name is assigned automatically as "mfr" followed by the number assigned to the bundle.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

This command can be entered only on the multilink Frame Relay bundle interface.

Note You can enter the **frame-relay multilink bid** command at any time without affecting the current state of the interface; however, the BID will not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

Only one BID is allowed per bundle. A later entry of the **frame-relay multilink bid** command supersedes prior entries.

The local and peer BIDs do not have to be unique.

Examples

The following example shows how to assign a BID of "bundle1" to the multilink Frame Relay bundle. The previous BID for the bundle was "mfr0."

```
interface mfr0
 frame-relay multilink bid bundle1
```

Related Commands

Command	Description
frame-relay multilink lid	Assigns a LID name to a multilink Frame Relay bundle link.
interface mfr	Configures a multilink Frame Relay bundle interface.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.
shutdown (interface)	Disables an interface.

frame-relay multilink hello

To configure the interval at which a bundle link will send out hello messages, use the **frame-relay multilink hello** command in interface configuration mode. To reset this value to the default setting, use the **no** form of this command.

frame-relay multilink hello *seconds*

no frame-relay multilink hello

Syntax Description

seconds	Interval, in seconds, at which a bundle link will send out hello messages. Range: 1 to 180. Default: 10.

Command Default

The interval is set at 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

The **frame-relay multilink hello** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Both ends of a bundle link send out hello messages at regular intervals. When a peer device receives a hello message, it responds by sending an acknowledgment. This exchange of hello messages and acknowledgments serves as a keepalive mechanism for the link. If the bundle link sends a hello message but does not receive an acknowledgment, it will resend the hello message up to a configured maximum number of times. If the bundle link exhausts the maximum number of retries, the bundle link line protocol is considered down (nonoperational).

The setting of the hello message interval on the local router is independent of the setting on the peer device.

Examples

The following example shows how to configure a bundle link to send hello messages every 15 seconds:

```
interface serial0
 encapsulation frame-relay mfr0
 frame-relay multilink hello 15
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink ack	Configures the number of seconds that a bundle link will wait for a hello message acknowledgment before resending the hello message.
frame-relay multilink retry	Configures the maximum number of times that a bundle link will resend a hello message while waiting for an acknowledgment.

frame-relay multilink lid

To assign a bundle link identification (LID) name to a multilink Frame Relay bundle link, use the **frame-relay multilink lid** command in interface configuration mode. To reset the name to the default, use the **no** form of this command.

frame-relay multilink lid *name*

no frame-relay multilink lid

Syntax Description

name	Bundle link identification (LID) name. The name can be up to 49 characters long. The default is the name of the physical interface.

Command Default

The name of the physical interface is used as the LID.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was implemented on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

The **frame-relay multilink lid** command can be configured only on bundle link interfaces that have been associated with a bundle using the **encapsulation frame-relay mfr** command.

Note You can enter the **frame-relay multilink lid** command at any time without affecting the current state of the interface; however, the LID will not go into effect until the interface has gone from the down state to the up state. One way to bring the interface down and back up again is by using the **shutdown** and **no shutdown** commands in interface configuration mode.

The LID will be used to identify the bundle link to peer devices and to enable the devices to identify which bundle links are associated with which bundles. The LID can also be assigned when the bundle link is created by using the **encapsulation frame-relay mfr** command with the *name* argument. If the LID is not assigned, the default LID is the name of the physical interface.

The local and peer LIDs do not have to be unique.

Examples

The following example shows the LID named BL1 assigned to serial interface 0:

```
interface serial 0
 encapsulation frame-relay mfr0
 frame-relay multilink lid BL1
```

Related Commands

Command	Description
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.
shutdown (interface)	Disables an interface.

frame-relay switching

To enable permanent virtual switching (PVC) switching on a Frame Relay DCE device or a Network-to-Network Interface (NNI), use the **frame-relay switching** command in global configuration mode. To disable switching, use the **no** form of this command.

frame-relay switching

no frame-relay switching

Syntax Description

This command has no arguments or keywords.

Defaults

Switching is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.

Usage Guidelines

You must add this command to the configuration file before configuring the routes.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, you do not need to configure the **frame-relay switching** command when configuring a Frame Relay interface as the DCE.

In Cisco IOS Release 12.2(31)SB, you must configure the **frame-relay switching** command when you configure a Frame Relay interface as the DCE.

Examples

The following example shows the command that is entered in the configuration file before the Frame Relay configuration commands to enable switching:

```
frame-relay switching
```

glbp authentication

To configure an authentication string for the Gateway Load Balancing Protocol (GLBP), use the **glbp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

no glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [**0** | **7**] *key* | **key-chain** *name-of-chain*}}

Syntax Description

group-number	GLBP group number in the range from 0 to 1023.
text *string*	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
md5	Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key string cannot exceed 100 characters in length. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
7	(Optional) Encrypted key.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No authentication of GLBP messages occurs.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	The **md5** keyword and associated parameters were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The same authentication method must be configured on all the routers that are configured to be members of the same GLBP group, to ensure interoperation. A router will ignore all GLBP messages that contain the wrong authentication information.

If password encryption is configured with the **service password-encryption** command, the software saves the key string in the configuration as encrypted text.

Examples

The following example configures stringxyz as the authentication string required to allow GLBP routers in group 10 to interoperate:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 authentication text stringxyz
```

In the following example, GLBP queries the key chain "AuthenticateGLBP" to obtain the current live key and key ID for the specified key chain:

```
Router(config)# key chain AuthenticateGLBP
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
service password-encryption	Encrypts passwords.

glbp forwarder preempt

To configure a router to take over as active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **glbp forwarder preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]

no glbp *group* **forwarder preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

Forwarder preemption is enabled with a default delay of 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows a router being configured to preempt the current AVF when the current AVF falls below its low weighting threshold. If the router preempts the current AVF, it waits 60 seconds before taking over the role of the AVF.

```
glbp 10 forwarder preempt delay minimum 60
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp ipv6

To activate the Gateway Load Balancing Protocol (GLBP) in IPv6, use the **glbp ipv6** command in interface configuration mode. To disable GLBP, use the **no** form of this command.

glbp *group* **ipv6** [*ipv6-address* | **autoconfig**]

no glbp *group* **ipv6** [*ipv6-address* | **autoconfig**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
ip-address	(Optional) Virtual IPv6 address for the GLBP group. The IPv6 address must be in the same subnet as the interface IPv6 address.
autoconfig	(Optional) Indicates a default IPv6 address can be created based on a MAC address.

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **glbp ipv6** command activates GLBP on the configured interface. If an IPv6 address is specified, that address is used as the designated virtual IPv6 address for the GLBP group. If no IPv6 address is specified, the designated address is learned from another router configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one router on the cable must have been configured with the designated address. A router must be configured with, or have learned, the virtual IPv6 address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ipv6** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IPv6 address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Examples

The following example enables GLBP on an IPv6 configured interface:

```
Router(config-if)# glbp ipv6
```

Related Commands

Command	Description
glbp ip	Activates the GLBP in IPv4.
show glbp	Displays GLBP information.

glbp load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **glbp load-balancing** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

glbp *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]

no glbp *group* **load-balancing**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
host-dependent	(Optional) Specifies a load balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
round-robin	(Optional) Specifies a load balancing method where each virtual forwarder in turn is included in address resolution replies for the virtual IP address. This method is the default.
weighted	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

Command Default

The round-robin method is the default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T2	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.0(1)M1	This command was modified. When the **no** form of this command is configured, if the AVG does not have an Active Virtual Forwarder (AVF), it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.1(2)T	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.

Usage Guidelines

Use the host-dependent method of GLBP load balancing when you need each host to always use the same router. Use the weighted method of GLBP load balancing when you need unequal load balancing because routers in the GLBP group have different forwarding capacities.

Examples

The following example shows the host-dependent load-balancing method being configured for the AVG of the GLBP group 10:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip 10.21.8.10
Router(config-if)# glbp 10 load-balancing host-dependent
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp name

To enable IP redundancy by assigning a name to the Gateway Load Balancing Protocol (GLBP) group, use the **glbp name** command in interface configuration mode. To disable IP redundancy for a group, use the **no** form of this command.

glbp *group-number* **name** *group-name*

no glbp *group-number* **name** *group-name*

Syntax Description

group-number	GLBP group number. Range is from 0 to 1023.
group-name	GLBP group name specified as a character string. Maximum number of characters is 255.

Defaults

IP redundancy for a group is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The GLBP redundancy client must be configured with the same GLBP group name so that the redundancy client and the GLBP group can be connected.

Examples

The following example assigns the abccomp name to GLBP group 10:

```
Router(config-if)# glbp 10 name abccomp
```

Related Commands

Command	Description
glbp authentication	Configures an authentication string for the GLBP.
glbp forwarder preempt	Configures a router to take over as AVF for a GLBP group if it has higher priority than the current AVF.
glbp ip	Activates GLBP.
glbp load-balancing	Specifies the load-balancing method used by the AVG of GLBP.

Command	Description
glbp preempt	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
glbp priority	Sets the priority level of the gateway within a GLBP group.
glbp timers	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.
glbp timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
glbp weighting	Specifies the initial weighting value of the GLBP gateway.
glbp weighting track	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
show glbp	Displays GLBP information.
track	Configures an interface to be tracked where the GLBP weighting changes based on the state of the interface.

glbp preempt

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has higher priority than the current AVG, use the **glbp preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp *group* **preempt** [**delay minimum** *seconds*]

no glbp *group* **preempt** [**delay minimum**]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

A GLBP router with a higher priority than the current AVG cannot assume the role of AVG.
The default delay value is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows a router being configured to preempt the current AVG when its priority of 254 is higher than that of the current AVG. If the router preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
Router(config-if)# glbp 10 preempt delay minimum 60
Router(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp priority	Sets the priority level of the router within a GLBP group.

glbp priority

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **glbp priority** command in interface configuration mode. To remove the priority level of the gateway, use the **no** form of this command.

glbp *group* **priority** *level*

no glbp *group* **priority** *level*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
level	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

Command Default

The GLBP virtual gateway preemptive scheme is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to control which virtual gateway becomes the active virtual gateway (AVG). After the priorities of several different virtual gateways are compared, the gateway with the numerically higher priority is elected as the AVG. If two virtual gateways have equal priority, the gateway with the higher IP address is selected.

Examples

The following example shows a virtual gateway being configured with a priority of 254:

```
Router(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp preempt	Configures a router to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

glbp timers

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

glbp *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*

no glbp *group* **timers**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
msec	(Optional) Specifies that the following (*hellotime* or *holdtime)* argument value will be expressed in milliseconds rather than seconds.
hellotime	Hello interval. The default is 3 seconds (3000 milliseconds).
holdtime	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The default is 10 seconds (10,000 milliseconds).

Command Default

GLBP timers are set to their default values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Routers on which timer values are not configured can learn timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All routers in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Normally, holdtime is greater than three times the value of hello time, (*holdtime* > 3 * *hellotime*). The range of values for holdtime force the holdtime to be greater than the hello time.

Examples

The following example shows the GLBP group 10 on Fast Ethernet interface 0/0 timers being configured for an interval of 5 seconds between hello packets, and the time after which virtual gateway and virtual forwarder information is considered to be invalid to 18 seconds:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip
Router(config-if)# glbp 10 timers 5 18
```

Related Commands

Command	Description
glbp ip	Activates GLBP.
show glbp	Displays GLBP information.

glbp timers redirect

To configure the time during which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF), use the **glbp timers redirect** command in interface configuration mode. To restore the redirect timers to their default values, use the **no** form of this command.

glbp *group* **timers redirect** *redirect timeout*

no glbp *group* **timers redirect** *redirect timeout*

Syntax Description

group	GLBP group number in the range from 0 to 1023.
redirect	The redirect timer interval in the range from 0 to 3600 seconds. The default is 600 seconds (10 minutes). **Note** The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.
timeout	The time interval, in the range from 600 to 64,800 seconds, before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Command Default

The GLBP redirect timers are set to their default values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. If the virtual forwarder has learned the virtual MAC address from hello messages, it is referred to as a secondary virtual forwarder.

The redirect timer sets the time delay between a forwarder failing on the network and the AVG assuming that the forwarder will not return. The virtual MAC address to which the forwarder was responsible for replying is still given out in Address Resolution Protocol (ARP) replies, but the forwarding task is handled by another router in the GLBP group.

Note The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.

The timeout interval is the time delay between a forwarder failing on the network and the MAC address for which the forwarder was responsible becoming inactive on all of the routers in the GLBP group. After the timeout interval, packets sent to this virtual MAC address will be lost. The timeout interval must be long enough to allow all hosts to refresh their ARP cache entry that contained the virtual MAC address.

Examples

The following example shows the commands used to configure GLBP group 1 on Fast Ethernet interface 0/0 with a redirect timer of 1800 seconds (30 minutes) and timeout interval of 28,800 seconds (8 hours):

```
Router# config terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# glbp 1 timers redirect 1800 28800
```

glbp weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **glbp weighting** command in interface configuration mode. To restore the default values, use the **no** form of this command.

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]

no glbp *group* **weighting**

Syntax Description

group	GLBP group number in the range from 0 to 1023.
maximum	Maximum weighting value in the range from 1 to 254. Default value is 100.
lower *lower*	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
upper *upper*	(Optional) Specifies an upper weighting value in the range from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

Command Default

The default gateway weighting value is 100 and the default lower weighting value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the router fails, the weighting value of the router may fall from the maximum value to below the lower threshold, causing the router to give up its role as a virtual forwarder. When the weighting value of the router rises above the upper threshold, the router can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to configure parameters for an interface to be tracked. If an interface on a router goes down, the weighting for the router can be reduced by a specified value.

Examples

The following example shows the weighting of the gateway for GLBP group 10 being set to a maximum of 110 with a lower weighting limit of 95 and an upper weighting limit of 105:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

Related Commands

Command	Description
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
track	Configures an interface to be tracked.

glbp weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **glbp weighting track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

glbp *group* **weighting track** *object-number* [**decrement** *value*]

no glbp *group* **weighting track** *object-number* [**decrement** *value*]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
object-number	Object number representing an item to be tracked. The valid range is 1 to 1000. Use the **track** command to configure the tracked object.
decrement *value*	(Optional) Specifies an amount by which the GLBP weighting for the router is decremented (or incremented) when the interface goes down (or comes back up). The value range is from 1 to 254, with a default value of 10.

Command Default

Objects are not tracked for GLBP weighting changes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

This command ties the weighting of the GLBP gateway to the availability of its interfaces. It is useful for tracking interfaces that are not configured for GLBP.

When a tracked interface goes down, the GLBP gateway weighting decreases by 10. If an interface is not tracked, its state changes do not affect the GLBP gateway weighting. For each GLBP group, you can configure a separate list of interfaces to be tracked.

The optional *value* argument specifies by how much to decrement the GLBP gateway weighting when a tracked interface goes down. When the tracked interface comes back up, the weighting is incremented by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface to be tracked.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, Fast Ethernet interface 0/0 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting track 1
Router(config-if)# glbp 10 weighting track 2 decrement 5
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
track	Configures an interface to be tracked.

graceful-restart

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-capable router, use the **graceful-restart** command in OSPF router configuration mode. To disable graceful restart, use the **no** form of this command.

graceful-restart [**restart-interval** *interval*]

no graceful-restart

Syntax Description

restart-interval *interval*	(Optional) Graceful-restart interval in seconds. The range is from 1 to 1800, and the default is 120.

Command Default

The GR feature is not enabled on GR-capable routers.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

The **graceful-restart** command can be enabled only on GR-capable routers.

Examples

The following examples enables graceful restart mode on a GR-capable router in IPv6 and IPv4:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restar
```

The following examples enables graceful restart mode on a GR-capable router in IPv6 only:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPFv3 graceful restart feature on a GR-aware router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

graceful-restart helper

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-aware router, use the **graceful-restart helper** command in OSPFv3 router configuration mode. To reset the router to its default, use the **no** form of this command.

graceful-restart helper {**disable** | **strict-lsa-checking**}

no graceful-restart helper

Syntax Description

disable	Disables graceful-restart-aware mode.
strict-lsa-checking	Enables graceful restart-helper mode with strict link-state advertisement (LSA) checking.

Command Default

Graceful restart-aware mode is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.

Usage Guidelines

GR-helper mode is configurable on both GR-aware and GR-capable routers; however, GR-aware routers can use only the **graceful-restart helper** command.

The **strict-lsa-checking** keyword indicates whether an OSPFv3 GR-aware router should terminate the helper function when there is a change to an LSA that would be flooded to the restarting router or when there is a changed LSA on the restarting router’s retransmission list when graceful restart is initiated.

Examples

The following example enables GR-helper mode with strict LSA checking:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart helper strict-lsa-checking
```

The following example shows how to enable GR-helper mode in an OSPFv3 IPv4 instance:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restart helper
```

RelatedCommands

Command	Description
graceful-restart	Enables the OSPFv3 GR feature on a graceful-restart-capable router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

group (IKE policy)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange (IKE) policy, which defines a set of parameters to be used during IKE negotiation, use the **group** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group {**1** | **2** | **5** | **14** | **15** | **16** | **19** | **20** | **24**}}

no group

Syntax Description

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group.

Command Default

DH group 1

Command Modes

ISAKMP policy configuration (config-isakmp)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.

Usage Guidelines

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

The ISAKMP group and the IPsec perfect forward secrecy (PFS) group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

Examples

The following example shows how to configure an IKE policy with the 1024-bit DH group (all other parameters are set to the defaults):

```
Router(config)# crypto isakmp policy 15
Router(config-isakmp) group 2
Router(config-isakmp) exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

hardware statistics

To enable the collection of hardware statistics, use the **hardware statistics** command in IPv6or IPv4 access-list configuration mode. To disable this feature, use the **no** form of this command.

hardware statistics

no hardware statistics

Syntax Description

This commands has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

IPv6 access-list configuration (config-ipv6-acl)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The hardware statistics command affects only global access-list (ACL) counters.

Examples

The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default secure hash algorithm (SHA)-1 hash algorithm, use the **no** form of this command.

hash {**sha** | **sha256** | **sha384** | **md5**}

no hash

Syntax Description

sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Defaults

The SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	IPv6 support was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.

Usage Guidelines

Use this command to specify the hash algorithm to be used in an IKE policy.

Examples

The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 hash md5
 exit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

home-address

To specify the mobile router home address using an IPv6 address or interface identifier, use the **home-address** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-address {**home-network** | *ipv6-address-identifier* | *interface*}

no home-address

SyntaxDescription

home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6-address-identifier	The IPv6 home address identifier.
interface	Specifies the interface to use to identify the home address.

Command Default

No IPv6 home address is specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **home-address** command allows you to specify the IPv6 home address. When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

home-network

To specify the home network's IPv6 prefix on the mobile router, use the **home-network** command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-network *ipv6-prefix*

no home-network

SyntaxDescription

ipv6-prefix	The IPv6 prefix of the home network.

Command Default

The IPv6 home network prefix is not specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Users can configure up to 10 home-network entries, and they are used in order of priority. The prefix identifies the home network of the mobile router and is used to discover when the mobile router is at home.

When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

The command syntax sorts the home networks by priority. The default priority is 128. The home networks will be tried from the smaller to the higher value and, for a same priority, the addresses without the discover keyword are tried first.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-address	Specifies the mobile router home address using an IPv6 address or interface identifier.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in router advertisement (RA) guard policy configuration mode.

hop-limit {**maximum** *limit* | **minimum** *limit*}

Syntax Description

maximum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is less than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

host group

To create a host group configuration in IPv6 Mobile, use the **host group** command in home agent configuration mode. To remove a host configuration, use the **no** form of this command.

host group *profile-name*

no host group *profile-name*

Syntax Description

profile-name	Specifies a name for the host group.

Command Default

No IPv6 Mobile host configurations exist.

Command Modes

Home agent configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **host group** command creates an IPv6 Mobile home-agent host configuration with a given profile name. Multiple instances with different profile names can be created and used.

Do not configure two separate groups with the same IPv6 address. For example, host group group1 and host group group2 cannot both be configured with the same IPv6 address of baba::1.

Examples

In the following example, the user enters home agent configuration mode and creates a host group named group1:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)# host group group1
```

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 Mobile node.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

hostname

To specify or modify the hostname for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is Router.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)M4	This command was integrated into Cisco IOS Release 15.0(1)M4 and support for numeric hostnames added.

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer.*

The name must also follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.

```
Router(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

A hostname of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names—Implementation and Specification*.

On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the hostname of “Router,” you will only see the following prompt (on most systems):

```
Router(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign hostnames of no more than nine characters.

The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **hostname**, results in incorrect translation:

```
Router(config)#
Router(config)#hostname \99
% Hostname contains one or more illegal characters.
```

Examples

The following example changes the hostname to “host1”:

```
Router(config)# hostname host1
host1(config)#
```

Related Commands

Command	Description
setup	Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces.

identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the **identity** command in IKEv2 keyring peer configuration mode. To remove the identity, use the **no** form of this command.

identity {**address** {*ipv4-address* | *ipv6-address*} | **fqdn** *name* | **email** *email-id* | **key-id** *key-id*}

no identity

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address to identify the peer.
fqdn *name*	Uses the Fully Qualified Domain Name (FQDN) to identify the peer.
email *email-id*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietary types to identify the peer.

Command Default

Identity types are not specified to a peer.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an e-mail ID, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session, and the initiator looks up keys during session startup.

Examples

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 or IPv6 address or the range of the peers in an IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

identity local

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the **identity local** command in IKEv2 profile configuration mode. To remove the identity, use the **no** form of this command.

identity local {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **fqdn** *fqdn-string* | **email** *e-mail-string* | **key-id** *opaque-string*}

no identity local

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address as the local identity.
dn	Uses the distinguished name as the local identity.
fqdn *fqdn-string*	Uses the Fully Qualified Domain Name (FQDN) as the local identity.
email *email-string*	Uses the e-mail ID as the local identity.
key-id *opaque-string*	Uses the proprietary type opaque string as the local identity.

Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6). If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.

Note You can configure one local IKEv2 identity type for a profile.

Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 10.0.0.1
```

The following example shows how to specify an IPv6 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

import dns-server

To import the Domain Name System (DNS) recursive name server option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import dns-server** command in IPv6 DHCP pool configuration mode. To remove the available DNS recursive name server list, use the **no** form of this command.

import dns-server

no import dns-server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS recursive name server list is not imported to a client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The DNS recursive name server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.

The DNS recursive name server list option code is 23. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import a list of available DNS recursive name servers to a client:

```
Router(config-dhcp)# import dns-server
```

Related Commands

Command	Description
import domain-name	Imports the domain search list option to a DHCP for IPv6 client.

import domain-name

To import the domain name search list option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name search list, use the **no** form of this command.

import domain-name

no import domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

The domain search list is not imported to the client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The domain name search list option specifies the domain search list the client is to use when resolving hostnames with DNS.

The domain name search list option code is 24. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import a domain search list to the client:

```
Router(config-dhcp)# import domain-name
```

Related Commands

Command	Description
import dns-server	Imports the DNS recursive name server option to a DHCP for IPv6 client.

import information refresh

To import the information refresh time option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import information refresh** command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

import information refresh

no import information refresh

Syntax Description

This command has no arguments or keywords.

Command Default

The information refresh time option is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCP for IPv6. It is used only in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the information refresh time:

```
import information refresh
```

Related Commands

Command	Description
information refresh	Specifies the information refresh time to be sent to the client.

import nis address

To import the network information service (NIS) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nis address

no import nis address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS servers option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS servers option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS address of an IPv6 server:

```
import nis address
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.

Command	Description
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name

no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the “DHCPv6 Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client’s NIS+ domain name information to the client.

import nisp address

To import the network information service plus (NIS+) servers option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nisp address

no import nisp address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS+ address of an IPv6 server:

```
import nisp address
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.

Command	Description
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name

no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the “DHCPv6 Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client’s NIS+ domain name information to the client.

import sip address

To import the Session Initiation Protocol (SIP) server IPv6 address list option to the outbound SIP proxy server, use the **import sip address** command in IPv6 DHCP pool configuration mode. To remove the SIP server IPv6 address list, use the **no** form of this command.

import sip address

no import sip address

Syntax Description

This command has no arguments or keywords.

Command Default

SIP IPv6 address list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server IPv6 address list option specifies a list of IPv6 addresses that indicate SIP outbound proxy servers available to the client. Servers must be listed in order of preference.

The SIP server IPv6 address list option code is 22. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example enables the user to import a SIP server IPv6 address list to the client:

```
Router(config-dhcp)# import sip address
```

Related Commands

Command	Description
import sip domain-name	Imports a SIP server domain-name list option to the outbound SIP proxy server.

import sip domain-name

To import a Session Initiation Protocol (SIP) server domain-name list option to the outbound SIP proxy server, use the **import sip domain-name** command in IPv6 DHCP pool configuration mode. To remove the SIP server domain-name list, use the **no** form of this command.

import sip domain-name

no import sip domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

SIP domain-name list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server domain-name list option contains the domain names of the SIP outbound proxy servers. Domain names must be listed in order of preference. The option may contain multiple domain names, but the client must try the records in the order listed. The client resolves the subsequent domain names only if attempts to contact the first one failed or yielded no common transport protocols between client and server or denoted a domain administratively prohibited by client policy.

The SIP server domain-name list option code is 21. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example enables the user to import a SIP server domain-name list to the client:

```
Router(config-dhcp)# import sip domain-name
```

Related Commands

Command	Description
import sip address	Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

import sntp address

To import the Simple Network Time Protocol (SNTP) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import sntp address** command in IPv6 DHCP pool configuration mode. To remove the SNTP server address, use the **no** form of the command.

import sntp address *ipv6-address*

no import sntp address *ipv6-address*

Syntax Description

ipv6-address	(Optional) The IPv6 address for SNTP. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No SNTP server address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

DHCP for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The SNTP address option can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to import the SNTP server address:

```
import sntp address
```

Related Commands

Command	Description
sntp address	Specifies the SNTP server to be sent to the client.

information refresh

To specify the information refresh time to be sent to the client, use the **information refresh** command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

information refresh {*days* [*hours minutes*] | **infinity**}

no information refresh {*days* [*hours minutes*] | **infinity**}

Syntax Description

days	Refresh time specified in number of days. The default is 0 0 86400, which equals 24 hours.
hours	(Optional) Refresh time specified in number of hours.
minutes	(Optional) Refresh time specified in number of minutes. The minimum refresh time that can be used is 0 0 600, which is 10 minutes.
infinity	Sets the IPv6 value of 0xffffffff used to configure the information refresh time to infinity.

Command Default

Information refresh information is not sent to the client. The client refreshes every 24 hours if no refresh information is sent.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The information refresh time option specifies the maximum time a client should wait before refreshing information retrieved from DHCP for IPv6. It is only used in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The maximum value for the information refresh period on the DHCP for IPv6 client is 7 days. The maximum value is not configurable.

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the “DHCP Options” appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the information refresh time to be 1 day, 1 hour, and 1 second:

```
information refresh 1 1 1
```

Related Commands

Command	Description
import information refresh	Imports the information refresh time option to a DHCP for IPv6 client.

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect [*parameter-map-name*]

no inspect [*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of a previously configured inspect parameter-map. If you do not specify a parameter map name, the software uses the default values for all the parameters.

Command Default

None

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

You can use this subcommand after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type** inspect commands.

To enable Cisco IOS stateful packet inspection, enter the name of an inspect parameter-map that was previously configured by using the **parameter-map type inspect** command.

This command lets you specify the attributes that will be used for the inspection.

Examples

The following example specifies inspection parameters for alert and audit-trail, and requests the **inspect** action with the specified parameters:

```
parameter-map type inspect insp-params
 alert on
 audit-trail on

policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect inspect-params
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates a Layer 3 or Layer 4 inspect type policy map.

interface mfr

To configure a multilink Frame Relay bundle interface, use the **interface mfr** command in global configuration mode. To remove the bundle interface, use the **no** form of this command.

interface mfr *number*

no interface mfr *number*

Syntax Description

number	Number that will uniquely identify this bundle interface. Range: 0 to 2147483647.

Command Default

A Frame Relay bundle interface is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was introduced on VIP-enabled Cisco 7500 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Frame Relay encapsulation is the default encapsulation type for multilink Frame Relay bundle interfaces.

A bundle interface is a virtual interface that serves as the Frame Relay data link and performs the same functions as a physical interface. The bundle is made up of physical serial links, called bundle links. The bundle links within a bundle function as one physical link and one pool of bandwidth. Functionality that you want to apply to the bundle links must be configured on the bundle interface.

The **no interface mfr** command will work only if all bundle links have been removed from the bundle by using the **no encapsulation frame-relay mfr** command.

Examples

The following example shows the configuration of a bundle interface called “mfr0.” The bundle identification (BID) name “BUNDLE-A” is assigned to the bundle. Serial interfaces 0 and 1 are assigned to the bundle as bundle links.

```
interface mfr0
 frame-relay multilink bid BUNDLE-A
!
interface serial0
 encapsulation frame-relay mfr0
!
interface serial1
 encapsulation frame-relay mfr0
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number* [**type** *virtual-template-type*]

no interface virtual-template *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.
type *virtual-template-type*	(Optional) Specifies the type of virtual template.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's default configuration was modified for SNMP and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Cisco 10000 Series Router

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the **keepalive** command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.
- Disable link-status event messaging using the **no logging event link-status** command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** *number* **subinterface** command.

In Cisco IOS Release 12.2(33)SB, the default configuration for the **virtual-template snmp** command was changed to **no virtual-template snmp**. This prevents large numbers of entries into the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs. If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

Cisco 10000 Series Router

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

Virtual Template with PPP Authentication Example

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

IPsec Virtual Template Example

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol (CDP) on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. **Note** If the secondary address is used for a VRF table configuration with the **vrf** keyword, the **vrf** keyword must be specified also.
vrf	(Optional) Name of the VRF table. The *vrf-name* argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(28)SB	The **vrf** keyword and *vrf-name* argument were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

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

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 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. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

Note If any router on a network segment uses a secondary address, all other devices 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 very quickly cause routing loops.

Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

In the following example, Ethernet interface 0/1 is configured to automatically classify the source IP address in the VRF table vrf1:

```
interface ethernet 0/1
 ip address 10.108.1.27 255.255.255.0
 ip address 10.31.7.17 255.255.255.0 secondary vrf vrf1
 ip vrf autoclassify source
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge-group	Assigns each network interface to a bridge group.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.
show route-map	Displays static and dynamic route maps.

ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

ip directed-broadcast [*access-list-number* | *extended access-list-number*]

no ip directed-broadcast [*access-list-number* | *extended access-list-number*]

Syntax Description

access-list-number	(Optional) Standard access list number in the range from 1 to 199. If specified, a broadcast must pass the access list to be forwarded.
extended access-list-number	(Optional) Extended access list number in the range from 1300 to 2699.

Command Default

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The default behavior changed to directed broadcasts being dropped.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A router that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is "exploded" as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

The **ip directed-broadcast** command controls the explosion of directed broadcasts when they reach their target subnets. The command affects only the final transmission of the directed broadcast on its ultimate destination subnet. It does not affect the transit unicast routing of IP directed broadcasts.

If **directed broadcast** is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet. If an access list has been configured with the **ip directed-broadcast** command, only directed broadcasts that are permitted by the access list in question will be forwarded; all other directed broadcasts destined for the interface subnet will be dropped.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

Note Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

Examples

The following example enables forwarding of IP directed broadcasts on Ethernet interface 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip directed-broadcast
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip-extension

To specify that IP extensions are included in a certificate request either for enrollment or generation of a certificate authority (CA) certificate for the Cisco IOS CA, use the **ip-extension** command in ca-trustpoint configuration mode. To remove a previously specified IP extension, use the **no** form of this command.

ip-extension [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*}

no ip-extension [**multicast** | **unicast**] {**inherit** [**ipv4** | **ipv6**] | **prefix** *ipaddress* | **range** *min-ipaddress max-ipaddress*}

Syntax Description

multicast	(Optional) Specifies that only multicast traffic, a subsequent address family identifier (SAFI), will be included in certificate requests. **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
unicast	(Optional) Specifies that only unicast traffic, a SAFI, will be included in certificate requests. **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
inherit	Specifies that IP addresses will be inherited from an issuer certificate. The issuer's certificate is first checked to find a certificate containing the address range or prefix. If no match is found, the certificate from the next issuer in the chain is checked, and so forth, up the certificate chain, recursively, until a match is located.
ipv4	(Optional) Specifies that only IPv4 addresses are inherited. **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.
ipv6	(Optional) Specifies that only IPv6 addresses are inherited. **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.

prefix *ipaddress*	Specifies the IP address prefix or a single IP address for either an IPv4 or IPv6 address. The IP address formats are: • A.B.C.D IPv4 address • A.B.C.D/nn IPv4 prefix • X:X:X:X::X IPv6 address • X:X:X:X::X/<0-128> IPv6 prefix
range	Specifies that there is a range of IP addresses.
min-ipaddress	The beginning IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Beginning IPv4 address in the range • X:X:X:X::X Beginning IPv6 address in the range
max-ipaddress	The ending IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Ending IPv4 address in the range • X:X:X:X::X Ending IPv6 address in the range

Command Default

No IP extensions will be included in a certificate request.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

The **ip-extension** command may be used to specify IP extensions for a public key infrastructure (PKI) server or client and may be issued one or more times, including multiple issuances with the **inherit**, **prefix**, and **range** keywords. For the inherit option, if the address family is not specified, both IPv4 and IPv6 addresses will be inherited. When the IPv4 or IPv6 address family is not specified for prefix or range, the address family will be determined from the address format.

Note It is recommended that you validate each **ip-extension** command line against your existing IP-extension configuration according to RFC 3779, verifying that IP address ranges do not overlap. The issue's certificate may not be available to validate the issuer's certificate for subsets of addresses.

Examples

The following example shows how to specify that multiple IP extensions are included in the server certificate request:

```
Router(ca-trustpoint)# ip-extension multicast prefix 10.64.0.0/11

! Only multicast traffic with the IPv4 prefix 10.64.0.0/11 will be included in certificate
requests.

Router(ca-trustpoint)# ip-extension prefix 2001:100:1::/48

! Multicast and unicast traffic with the IPv6 prefix 2001:100:1::/48 will be included in
certificate requests.

Router(ca-trustpoint)# ip-extension inherit

! Multicast and unicast traffic with IPv4 and IPv6 addresses will be inherited from the
issuer's certificate.

Router(ca-trustpoint)# ip-extension inherit ipv6

! Multicast and unicast traffic with IPv6 addresses only will be inherited from the
issuer's certificate.

Router(ca-trustpoint)# ip-extension unicast range 209.165.200.225 143.255.55.255

! Unicast traffic within the specified IPv4 address range will be included in the
certificate request.

Router(ca-trustpoint)# ip-extension range 2001:1:1::1 2001:1:2:ffff:ffff:ffff:ffff:ffff

! Multicast and unicast traffic within the specified IPv6 address range will be included
in the certificate request.
```

The following is sample output from the **show crypto pki certificates verbose** command. The output displays X.509 certificate IP address extension information where the IPv4 multicast prefix has been set to 10.64.0.0/11, and the IPv4 unicast range has been set to 209.165.201.1 209.165.201.30.

```
CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number (hex): 01
   Certificate Usage: Signature
   Issuer:
     cn=srtr1
   Subject:
     cn=srtr1
   Validity Date:
     start date: 21:50:11 PST Sep 29 2008
     end   date: 21:50:11 PST Sep 29 2011
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (1024 bit)
   Signature Algorithm: MD5 with RSA Encryption
   Fingerprint MD5: 30C1C9B6 BC17815F DF6095CD EDE2A5F3
   Fingerprint SHA1: A67C451E 49E94E87 8EB0F71D 5BE642CF C68901EF
   X509v3 extensions:
     X509v3 Key Usage: 86000000
       Digital Signature
       Key Cert Sign
       CRL Signature
     X509v3 Subject Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
```

```
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
    Authority Info Access:
    X509v3 IP Extension:
        IPv4 (Unicast):
          209.165.202.129-209.165.202.158
        IPv4 (Multicast):
          10.64.0.0/11
  Associated Trustpoints: srtr1
```

Related Commands

Command	Description
show crypto pki certificates	Displays information about the CA certificate.
show crypto pki trustpoints	Displays information about trustpoints that are configured on the router.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, use the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

ip http server

no ip http server

Syntax Description

This command has no arguments or keywords.

Command Default

The HTTP server is disabled on the Cisco Catalyst 4000 series switch. The HTTP server is enabled for clustering on the following Cisco switches: Catalyst 3700 series, Catalyst 3750 series, Catalyst 3550 series, Catalyst 3560 series, and Catalyst 2950 series.

The HTTP server uses the standard port 80 by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(2)T	IPv6 support was added.
12.2(15)T	The HTTP 1.0 implementation was replaced by the HTTP 1.1 implementation. The secure HTTP server feature was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

With IPv6 support added in Cisco IOS Release 12.2(2)T, the **ip http server** command simultaneously enables and disables both IP and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command will only be applied to IPv4 traffic. IPv6 traffic filtering is not supported.

Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

Examples

The following example shows how to enable the HTTP server on both IP and IPv6 systems:

```
Router(config)# ip http server
Router(config)# ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.
ip http secure-server	Enables the HTTPS server.