router-id (IPv6)

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) for IPv6 to use the previous OSPF for IPv6 router ID behavior, use the **no** form of this command.

router-id {*router-id*}

no router-id {*router-id*}

Syntax Description

router-id	Router ID for this OSPF process.

Command Default

The router ID is chosen automatically.

Command Modes

Router configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(6)T	Support for Enhanced Internal Gateway Routing Protocol (EIGRP) IPv6 was added.
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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

OSPF for IPv6 (or OSPF version 3, or OSPFv3) is backward-compatible with OSPF version 2. In OSPFv3 and OSPF version 2, the router uses the 32-bit IPv4 address to select the router ID for an OSPF process. If an IPv4 address exists when OSPFv3 is enabled on an interface, then that IPv4 address is used for the router ID. If more than one IPv4 address is available, a router ID is chosen using the same rules as for OSPF version 2. If no IPv4 addresses are configured, the router selects a router ID automatically. Each router ID must be unique.

If this command is used on an OSPF for IPv6 router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPFv3 process restart. To manually restart the OSPFv3 process, use the **clear ipv6 ospf process** command.

Examples

The following example specifies a fixed router ID:

```
Router(config-rtr)# router-id 10.1.1.1
```

Related Commands

Command	Description
clear ipv6 ospf	Clears the OSPF for IPv6 state based on the OSPF routing process ID.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
ipv6 router ospf	Enables OSPF for IPv6 router configuration mode.

router-id (OSPFv3)

To use a fixed router ID, use the **router-id** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To force OSPFv3 to use the previous OSPFv3 router ID behavior in IPv4, use the **no** form of this command.

router-id {*router-id*}

no router-id {*router-id*}

Syntax Description

router-id	Router ID for this OSPFv3 process.

Command Default

The router ID is chosen automatically.

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

OSPFv3 is backward-compatible with OSPF version 2. In OSPFv3 and OSPF version 2, the router uses the 32-bit IPv4 address to select the router ID for an OSPFv3 process. If an IPv4 address exists when OSPFv3 is enabled on an interface, then that IPv4 address is used for the router ID. If more than one IPv4 address is available, a router ID is chosen using the same rules as for OSPF version 2. If no IPv4 addresses are configured, the router selects a router ID automatically. Each router ID must be unique.

If this command is used on an OSPFv3 router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPFv3 process restart.

Examples

The following example specifies a fixed router ID:

```
Router(config-router)# router-id 10.1.1.1
```

Related Commands

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

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in router advertisement (RA) guard policy configuration mode:

router-preference maximum {**high** | **low** | **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

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

Usage Guidelines

The **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default router advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised **default router preference** is set to **high** in the received packet, then packet is dropped. If the command option is set to **medium** or **low** in the received packet, then packet is not dropped.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures router-preference maximum verification to be high:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-nd-inspection)# router-preference maximum high
```

Related Commands

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

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **route-target** command in VRF configuration or in VRF address family configuration mode. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target [**import** | **export** | **both**] *route-target-ext-community*

no route-target [**import** | **export** | **both**] [*route-target-ext-community*]

Syntax Description

import	(Optional) Imports routing information from the target VPN extended community.
export	(Optional) Exports routing information to the target VPN extended community.
both	(Optional) Imports both import and export routing information to the target VPN extended community.
route-target-ext-community	The route-target extended community attributes to be added to the VRF's list of import, export, or both (import and export) route-target extended communities.

Command Default

A VRF has no route-target extended community attributes associated with it.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
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)SRB	This command was modified. Support for IPv6 was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers was changed to asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The **route-target** command creates lists of import and export route-target extended communities for the specified VRF. Enter the command one time for each target community. Learned routes that carry a specific route-target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route target specifies a target VPN extended community. Like a route distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

- *16-bit autonomous-system-number***:***your 32-bit number*
  For example, 101:3.
- *32-bit IP address***:***your 16-bit number*
  For example, 192.168.122.15:1.

Note In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how to configure route-target extended community attributes for a VRF in IPv4. The result of the command sequence is that VRF named vrf1 has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 10.27.0.130:200):

```
ip vrf vrf1
 route-target both 1000:1
 route-target export 1000:2
 route-target import 10.27.0.130:200
```

The following example shows how to configure route-target extended community attributes for a VRF that includes IPv4 and IPv6 address families:

```
vrf definition site1
rd 1000:1
address-family ipv4
 route-target export 100:1
 route-target import 100:1
address-family ipv6
 route-target export 200:1
 route-target import 200:1
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asplain format—65537—and how to set the route target to extended community value 65537:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 65537:100
 exit
route-map vrf1 permit 10
 set extcommunity rt 65537:100
 end
```

After the configuration is completed, use the **show route-map** command to verify that the extended community is set to the route target containing the 4-byte autonomous system number of 65537:

```
Router# show route-map vrf1

route-map vrf1, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:65537:100
  Policy routing matches: 0 packets, 0 bytes
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route target that uses a 4-byte autonomous system number in asdot format—1.1—and how to set the route target to extended community value 1.1:100 for routes that are permitted by the route map:

```
ip vrf vrf1
 rd 64500:100
 route-target both 1.1:100
 exit
```

```
route-map vrf1 permit 10
 set extcommunity rt 1.1:100
 end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets Border Gateway Protocol (BGP) connections using hard or soft reconfiguration.
import map	Configures an import route map for a VRF.
ip vrf	Configures a VRF routing table.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.

rsakeypair

To specify which Rivest, Shamir, and Adelman (RSA) key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

rsakeypair *key-label* [*key-size* [*encryption-key-size*]]

Syntax Description

key-label	Name of the key pair, which is generated during enrollment if it does not already exist or if the **auto-enroll regenerate** command is configured.
key-size	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key pair. If the size is not specified, the existing key size is used.
encryption-key-size	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Defaults

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
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) command was added.

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair “exampleCAkeys”:

```
crypto ca trustpoint exampleCAkeys
 enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

sccp ccm

To add a Cisco Unified Communications Manager server to the list of available servers and set various parameters—including IP address or Domain Name System (DNS) name, port number, and version number—use the **sccp ccm** command in global configuration mode. To remove a particular server from the list, use the **no** form of this command.

NM-HDV or NM-HDV-FARM Voice Network Modules

sccp ccm {*ipv4-address* | *ipv6-address* | *dns*} **priority** *priority* [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]

no sccp ccm {*ipv4-address* | *ipv6-address* | *dns*}

NM-HDV2 or NM-HD-1V/2V/2VE Voice Network Modules

sccp ccm {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]

no sccp ccm {*ipv4-address* | *ipv6-address* | *dns*}

Syntax Description

ipv4-address	IPv4 address of the Cisco Unified Communications Manager server.
ipv6-address	IPv6 address of the Cisco Unified Communications Manager server.
dns	DNS name.
identifier *identifier-number*	Specifies the number that identifies the Cisco Unified Communications Manager server. The range is 1 to 65535.
priority *priority*	Specifies the priority of this Cisco Unified Communications Manager server relative to other connected servers. The range is 1 (highest) to 4 (lowest). **Note** This keyword is required only for NM-HDV and NM-HDV-FARM modules. Do not use this keyword if you are using the NM-HDV2 or NM-HD-1V/2V/2VE; set the priority using the **associate ccm** command in the Cisco Unified Communications Manager group.
port *port-number*	(Optional) Specifies the TCP port number. The range is 1025 to 65535. The default is 2000.
version *version-number*	(Optional) Cisco Unified Communications Manager version. Valid versions are **3.0**, **3.1**, **3.2**, **3.3**, **4.0**, **4.1**, **5.0.1**, **6.0**, and **7.0+**. There is no default value.
trustpoint	(Optional) Specifies the trustpoint for Cisco Unified Communications Manager certificate.
label	Cisco Unified Communications Manager trustpoint label.

Command Default

The default port number is 2000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.3(8)T	This command was modified. The **identifier** keyword and additional values for Cisco Unified Communications Manager versions were added.
12.4(11)XW	This command was modified. The **6.0** keyword was added to the list of version values.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. Support for IPv6 was added. The **version** keyword and *version-number* argument were changed from being optional to being required, and the **7.0+** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **trustpoint** keyword and the *label* argument were added.

Usage Guidelines

You can configure up to four Cisco Unified Communications Manager servers—a primary and up to three backups—to support digital signal processor (DSP) farm services. To add the Cisco Unified Communications Manager server to a Cisco Unified Communications Manager group, use the **associate ccm** command.

IPv6 support is provided for registration with Cisco Unified CM version 7.0 and later.

To enable Ad Hoc or Meet-Me hardware conferencing in Cisco Unified CME, you must first set the **version** keyword to **4.0** or a later version.

Beginning with Cisco IOS Release 12.4(22)T users manually configuring the **sccp ccm** command must provide the version. Existing router configurations are not impacted because automatic upgrade and downgrade are supported.

Examples

The following example shows how to add the Cisco Unified Communications Manager server with IP address 10.0.0.0 to the list of available servers:

```
Router(config)# sccp ccm 10.0.0.0 identifier 3 port 1025 version 4.0
```

The following example shows how to add the Cisco Unified CallManager server whose IPv6 address is 2001:DB8:C18:1::102:

```
Router(config)# sccp ccm 2001:DB8:C18:1::102 identifier 2 version 7.0
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
sccp ccm group	Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode.

Command	Description
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.
show sccp	Displays SCCP configuration information and current status.

sccp ccm group

To create a Cisco Unified Communications Manager group and enter SCCP Cisco CallManager configuration mode, use the **sccp ccm group** command in global configuration mode. To remove a particular Cisco Unified Communications Manager group, use the **no** form of this command.

sccp ccm group *group-number*

no sccp ccm group *group-number*

Syntax Description

group-number	Number that identifies the Cisco Unified Communications Manager group. Range is 1 to 50.

Command Default

No groups are defined, so all servers are configured individually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The group number range was increased to 50.

Usage Guidelines

Use this command to group Cisco Unified Communications Manager servers that are defined using the **sccp ccm** command. You can associate designated DSP farm profiles using the **associate profile** command so that the DSP services are controlled by the Cisco Unified Communications Manager servers in the group.

Examples

The following example enters SCCP Cisco CallManager configuration mode and associates Cisco Unified Communications Manager 25 with Cisco Unified Communications Manager group 10:

```
Router(config)# sccp ccm group 10
Router(config-sccp-ccm)# associate ccm 25 priority 2
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco Unified Communications Manager group.
bind interface	Binds an interface with a Cisco Unified Communications Manager group.

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager connections fails.
sccp ccm	Adds a Cisco Unified Communications Manager server to the list of available servers.

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*

no sec-level minimum *value*

Syntax Description

value	Sets the minimum security level, which is a value from 1 through 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

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 **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** 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 specify 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

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.

self-identity

To define the identity that the local Internet Key Exchange (IKE) uses to identify itself to the remote peer, use the **self-identity** command in ISAKMP profile configuration mode. To remove the Internet Security Association and Key Management Protocol (ISAKMP) identity that was defined for the IKE, use the **no** form of this command.

self-identity {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}

no self-identity {**address** | **address ipv6**] | **fqdn** | **user-fqdn** *user-fqdn*}

Syntax Description

address	The IP address of the local endpoint.
address ipv6	The IPv6 address of the local endpoint.
fqdn	The fully qualified domain name (FQDN) of the host.
user-fqdn *user-fqdn*	The user FQDN that is sent to the remote endpoint.

Command Default

If no ISAKMP identity is defined in the ISAKMP profile configuration, global configuration is the default.

Command Modes

ISAKMP profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	The **address ipv6** keyword was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example shows that the IKE identity is the user FQDN "user@vpn.com":

```
crypto isakmp profile vpnprofile
 self-identity user-fqdn user@vpn.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in key chain key configuration mode. To revert to the default value, use the **no** form of this command.

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime [*start-time* {**infinite** | *end-time* | **duration** *seconds*}]

Syntax Description

start-time	Beginning time that the key specified by the **key** command is valid to be sent. The syntax can be either of the following: *hh*:*mm*:*ss Month date year* *hh*:*mm*:*ss date Month year* • *hh*—hours • *mm*—minutes • *ss*—seconds • *Month*—first three letters of the month • *date*—date (1–31) • *year*—year (four digits) The default start time and the earliest acceptable date is January 1, 1993.
infinite	Key is valid to be sent from the *start-time* value on.
end-time	Key is valid to be sent from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
duration *seconds*	Length of time (in seconds) that the key is valid to be sent.

Command Default

Forever (the starting time is January 1, 1993, and the ending time is infinite)

Command Modes

Key chain key configuration (config-keychain-key)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
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.

Usage Guidelines

Specify a *start-time* value and one of the following values: **infinite**, *end-time*, or **duration** *seconds*.

We recommend running Network Time Protocol (NTP) or some other time synchronization method if you intend to set lifetimes on keys.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

Examples

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# interface ethernet 0
Router(config-if)# ip rip authentication key-chain chain1
Router(config-if)# ip rip authentication mode md5
!
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
!
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named chain1 for EIGRP address-family. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences.

```
Router(config)# 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)# af-interface ethernet0/0
Router(config-router-af-interface)# authentication key-chain trees
Router(config-router-af-interface)# authentication mode md5
Router(config-router-af-interface)# exit
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# key chain chain1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string key1
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
Router(config-keychain-key)# exit
Router(config-keychain)# key 2
Router(config-keychain-key)# key-string key2
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
show key chain	Displays authentication key information.

send-nat-address

To send a client's post-Network Address Translation (NAT) address to the TACACS+ server, use the **send-nat-address** command in TACACS+ server configuration mode. To disable sending the post-NAT address, use the **no** form of this command.

send-nat-address

no send-nat-address

Syntax Description

This command has no arguments or keywords.

Command Default

The post-NAT address is not sent.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

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

Usage Guidelines

Use the **send-nat-address** command to send a client's post-NAT address to the TACACS+ server.

Examples

The following example shows how to send a client's post-NAT address to the TACACS+ server:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# send-nat-address
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.

serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]

no serial-number

Syntax Description

none	(Optional) Specifies that a serial number will not be included in the certificate request.

Defaults

Not configured. You will be prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was introduced.

Usage Guidelines

Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to omit a serial number from the “root” certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 ip-address none
 fqdn none
 serial-number none
 subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US

crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name** command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*

no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

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

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

Command	Description
aaa group server tacacs	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout *seconds*	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used.

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between Virtual Route Forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Note If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private** (RADIUS) command.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
 server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
 server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users logging into a Cisco network access server (NAS) to select a RADIUS server for authentication.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private {*ip-address* | *name* | *ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]

no server-private

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
name	Name of the private RADIUS or TACACS+ server host.
ipv6-address	IPv6 address of the private RADIUS or TACACS+ server host.
nat	(Optional) Specifies the port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
timeout *seconds*	(Optional) Specifies a timeout value. This value overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
key [**0** | **7**]	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global **tacacs-server key** command for this server only. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 7 is entered, the string that is entered is considered to be encrypted text.
string	(Optional) Character string specifying the authentication and encryption key.

Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.2S	This command was modified. The *ipv6-address* argument was added.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "TACACS+" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco

  ip vrf cisco
   rd 100:1

  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
tacacs-server host	Specifies a TACACS+ server host.

service pad

To enable all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers, use the **service pad** command in global configuration mode. To disable this service, use the **no** form of this command.

service pad [**cmns**] [**from-xot**] [**to-xot**]

no service pad [**cmns**] [**from-xot**] [**to-xot**]

Syntax Description

cmns	(Optional) Specifies sending and receiving PAD calls over CMNS.
from-xot	(Optional) Accepts XOT to PAD connections.
to-xot	(Optional) Allows outgoing PAD calls over XOT.

Command Default

All PAD commands and associated connections are enabled. PAD services over XOT or CMNS are not enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **cmns** 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The keywords **from-xot** and **to-xot** enable PAD calls to destinations that are not reachable over physical X.25 interfaces, but instead over TCP tunnels. This feature is known as PAD over XOT (X.25 over TCP).

Examples

If the **service pad** command is disabled, the **pad** EXEC command and all PAD related configurations, such as X.29, are unrecognized, as shown in the following example:

```
Router(config)# no service pad
Router(config)# x29 ?
% Unrecognized command
Router(config)# exit
Router# pad ?
% Unrecognized command
```

If the **service pad** command is enabled, the **pad** EXEC command and access to an X.29 configuration are granted as shown in the following example:

```
Router# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# service pad
Router(config)# x29 ?
access-list       Define an X.29 access list
inviteclear-time  Wait for response to X.29 Invite Clear message
profile           Create an X.3 profile
Router# pad ?
WORD   X121 address or name of a remote system
```

In the following example, PAD services over CMNS are enabled:

```
! Enable CMNS on a nonserial interface
interface ethernet0
 cmns enable
!
!Enable inbound and outbound PAD over CMNS service
service pad cmns
!
! Specify an X.25 route entry pointing to an interface’s CMNS destination MAC address
x25 route ^2193330 interface Ethernet0 mac 00e0.b0e3.0d62

Router# show x25 vc

SVC 1,  State: D1,  Interface: Ethernet0
     Started 00:00:08, last input 00:00:08, output 00:00:08

     Line: 0   con 0    Location: console Host: 2193330
      connected to 2193330 PAD <--> CMNS Ethernet0 00e0.b0e3.0d62

     Window size input: 2, output: 2
     Packet size input: 128, output: 128
     PS: 2  PR: 3  ACK: 3  Remote PR: 2  RCNT: 0  RNR: no
     P/D state timeouts: 0  timer (secs): 0
     data bytes 54/19 packets 2/3 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

Related Commands

Command	Description
cmns enable	Enables the CMNS on a nonserial interface.
show x25 vc	Displays information about active SVCs and PVCs.
x29 access-list	Limits access to the access server from certain X.25 hosts.
x29 profile	Creates a PAD profile script for use by the translate command.

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description

This command has no arguments or keywords.

Command Default

No passwords are encrypted.

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(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.

Caution This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples

The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
key-string (authentication)	Specifies the authentication string for a key.
neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

service-policy type inspect

To attach a firewall policy map to a zone-pair, use the **service-policy type inspect** command in zone-pair configuration mode. To disable this attachment to a zone-pair, use the **no** form of this command.

service-policy type inspect *policy-map-name*

no service-policy type inspect *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Zone-pair configuration (config-sec-zone-pair)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Use the **service-policy type inspect** command to attach a policy-map and its associated actions to a zone-pair.

Enter the command after entering the **zone-pair security** command.

Examples

The following example defines zone-pair z1-z2 and attaches the service policy p1 to the zone-pair:

```
!
zone security z1
zone security z2
!
class-map type inspect match-all c1
 match protocol tcp
policy-map type inspect p1
 class type inspect c1
  inspect
!
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
!
```

Related Commands

Command	Description
zone-pair security	Creates a zone-pair.

service timestamps

To configure the system to apply a time stamp to debugging messages or system logging messages, use the **service timestamps** command in global configuration mode. To disable this service, use the **no** form of this command.

service timestamps [**debug** | **log**] [**uptime** | **datetime** [**msec**]] [**localtime**] [**show-timezone**] [**year**]

no service timestamps [**debug** | **log**]

Syntax Description

debug	(Optional) Indicates time-stamping for debugging messages.
log	(Optional) Indicates time-stamping for system logging messages.
uptime	(Optional) Specifies that the time stamp should consist of the time since the system was last rebooted. For example "4w6d" (time since last reboot is 4 weeks and 6 days). • This is the default time-stamp format for both debugging messages and logging messages. • The format for uptime varies depending on how much time has elapsed: – *HHHH*:*MM*:*SS* (*HHHH* hours: *MM* minutes: *SS* seconds) for the first 24 hours – *D*d*HH*h (*D* days *HH* hours) after the first day – *W*w*D*d (*W* weeks *D* days) after the first week
datetime	(Optional) Specifies that the time stamp should consist of the date and time. • The time-stamp format for **datetime** is MMM DD HH:MM:SS, where MMM is the month, DD is the date, HH is the hour (in 24-hour notation), MM is the minute, and SS is the second. • If the **datetime** keyword is specified, you can optionally add the **msec localtime**, **show-timezone**, or **year** keywords. • If the **service timestamps datetime** command is used without addtional keywords, time stamps will be shown using UTC, without the year, without milliseconds, and without a time zone name.
msec	(Optional) Includes milliseconds in the time stamp, in the format *HH*:*DD*:*MM*:*SS*.*mmm*, where *.mmm* is milliseconds
localtime	(Optional) Time stamp relative to the local time zone.
year	(Optional) Include the year in the date-time format.
show-timezone	(Optional) Include the time zone name in the time stamp. **Note** If the **localtime** keyword option is not used (or if the local time zone has not been configured using the **clock timezone** command), time will be displayed in Coordinated Universal Time (UTC).

Command Default

Time stamps are applied to debug and logging messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.3(5)	Service time stamps are enabled by default.
12.3(1)	The **year** keyword was added.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Time stamps can be added to either debugging messages (**service timestamp debug**) or logging messages (**service timestamp log**) independently.

If the **service timestamps** command is specified with no arguments or keywords, the default is **service timestamps debug uptime**.

The **no service timestamps** command by itself disables time stamps for both debug and log messages.

The **uptime** form of the command adds time stamps (such as "2w3d") that indicating the time since the system was rebooted. The **datetime** form of the command adds time stamps (such as "Sep 5 2002 07:28:20") that indicate the date and time according to the system clock.

Entering the **service timestamps** {**debug** | **log**} command a second time will overwrite any previously configured **service timestamp** {**debug** | **log**} commands and associated options.

To set the local time zone, use the **clock timezone** *zone hours-offset* command in global configuration mode.

The time stamp will be preceeded by an asterisk or period if the time is potentially inaccurate. Table 49 describes the symbols that proceed the time stamp.

Table 49 Time-Stamping Symbols for syslog Messages

Symbol	Description	Example
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
*	Time is not authoritative: the software clock has not been set, or is not in sync with configured Network Time Protocol (NTP) servers.	*15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but the NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers.	.15:29:03.158 UTC Tue Feb 25 2003:

Examples

In the following example, the router begins with time-stamping disabled. Then, the default time-stamping is enabled (uptime time stamps applied to debug output). Then, the default time-stamping for logging is enabled (uptime time stamps applied to logging output).

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

no service timestamps debug uptime
no service timestamps log uptime

Router# config terminal
Router(config)# service timestamps
! issue the show running-config command in config mode using do
Router(config)# do show running-config | inc time
! shows that debug timestamping is enabled, log timestamping is disabled

service timestamps debug uptime
no service timestamps log uptime

! enable timestamps for logging messages
Router(config)# service timestamps log
Router(config)# do show run | inc time

service timestamps debug uptime
service timestamps log uptime

Router(config)# service sequence-numbers
Router(config)# end
000075: 5w0d: %SYS-5-CONFIG_I: Configured from console by console

! The following is a level 5 system logging message
! The leading number comes from the service sequence-numbers command.
! 4w6d indicates the timestamp of 4 weeks, 6 days

000075: 4w6d: %SYS-5-CONFIG_I: Configured from console by console
```

In the following example, the user enables time-stamping on logging messages using the current time and date in Coordinated Universal Time/Greenwich Mean Time (UTC/GMT), and enables the year to be shown.

```
Router(config)#
! The following line shows the timestamp with uptime (1 week 0 days)

1w0d: %SYS-5-CONFIG_I: Configured from console by console

Router(config)# service timestamps log datetime show-timezone year
Router(config)# end

! The following line shows the timestamp with datetime (11:13 PM March 22nd)

.Mar 22 2004 23:13:25 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows the change from UTC to local time:

```
Router# configure terminal

! Logging output can be quite long; first changing line width to show full
! logging message

Router(config)# line 0
Router(config-line)# width 180
Router(config-line)# logging synchronous
Router(config-line)# end
```

```
! Timestamping already enabled for logging messages; time shown in UTC.
Oct 13 23:20:05 UTC: %SYS-5-CONFIG_I: Configured from console by console

Router# show clock

23:20:53.919 UTC Wed Oct 13 2004

Router# configure terminal

Enter configuration commands, one per line.  End with the end command.

! Timezone set as Pacific Standard Time, with an 8 hour offset from UTC

Router(config)# clock timezone PST -8

Router(config)#

Oct 13 23:21:27 UTC: %SYS-6-CLOCKUPDATE:
System clock has been updated from 23:21:27 UTC Wed Oct 13 2004
to 15:21:27 PST Wed Oct 13 2004, configured from console by console.

Router(config)#
! Pacific Daylight Time (PDT) configured to start in April and end in October.
! Default offset is +1 hour.

Router(config)# clock summer-time PDT recurring first Sunday April 2:00 last Sunday
October 2:00

Router(config)#

! Time changed from 3:22 P.M. Pacific Standard Time (15:22 PST)
! to 4:22 P.M. Pacific Daylight (16:22 PDT)

Oct 13 23:22:09 UTC: %SYS-6-CLOCKUPDATE:
System clock has been updated from 15:22:09 PST Wed Oct 13 2004
to 16:22:09 PDT Wed Oct 13 2004, configured from console by console.

! Change the timestamp to show the local time and timezone.

Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# end

Oct 13 16:23:19 PDT: %SYS-5-CONFIG_I: Configured from console by console

Router# show clock
16:23:58.747 PDT Wed Oct 13 2004
Router# config t
Enter configuration commands, one per line.  End with the end command.
Router(config)# service sequence-numbers
Router(config)# end
Router#
```

In the following example, the **service timestamps log datetime** command is used to change previously configured options for the date-time time stamp.

```
Router(config)# service timestamps log datetime localtime show-timezone

Router(config)# end

! The year is not displayed.

Oct 13 15:44:46 PDT: %SYS-5-CONFIG_I: Configured from console by console

Router# config t
```

```
Enter configuration commands, one per line.  End with the end command.
Router(config)# service timestamps log datetime show-timezone year
Router(config)# end

! note: because the localtime option was not specified again, that option is
! removed from the output, and time is displayed in UTC (the default)

Oct 13 2004 22:45:31 UTC: %SYS-5-CONFIG_I: Configured from console by console
```

Related Commands

Command	Description
clock set	Manually sets the system clock.
ntp	Controls access to the system's NTP services.
service sequence-numbers	Stamps system logging messages with a sequence number.

session protocol (dial peer)

To specify a session protocol for calls between local and remote routers using the packet network, use the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**aal2-trunk** | **cisco** | **sipv2** | **smtp**}

no session protocol

Syntax Description

aal2-trunk	Dial peer uses ATM adaptation layer 2 (AAL2) nonswitched trunk session protocol.
cisco	Dial peer uses the proprietary Cisco VoIP session protocol.
sipv2	Dial peer uses the Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP). Use this keyword with the SIP option.
smtp	Dial peer uses Simple Mail Transfer Protocol (SMTP) session protocol.

Command Default

No default behaviors or values

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP peers on the Cisco 3600 series.
12.0(3)XG	This command was modified to support VoFR) dial peers.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300.
12.1(1)XA	This command was implemented for VoATM dial peers on the Cisco MC3810. The **aal2-trunk** keyword was added.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **sipv2** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release. The **aal2-trunk** and **smtp** keywords are not supported on the Cisco 7200 series in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

The **cisco** keyword is applicable only to VoIP on the Cisco 1750, Cisco 1751, Cisco 3600 series, and Cisco 7200 series routers.

The **aal2-trunk** keyword is applicable only to VoATM on the Cisco 7200 series router.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example shows that AAL2 trunking has been configured as the session protocol:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example shows that Cisco session protocol has been configured as the session protocol:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example shows that a VoIP dial peer for SIP has been configured as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

session target (VoIP dial peer)

To designate a network-specific address to receive calls from a VoIP or VoIPv6 dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1751, Cisco 3725, Cisco 3745, and Cisco AS5300

session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**$s$.** | **$d$.** | **$e$.** | **$u$.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **sip-server** | **registrar**} [**:***port*]

no session target

Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, and Cisco AS5850

session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**$s$.** | **$d$.** | **$e$.** | **$u$.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **settlement** *provider-number* | **sip-server** | **registrar**} [**:***port*]

no session target

Syntax Description

dhcp	Configures the router to obtain the session target via DHCP. **Note** The **dhcp** option can be made available only if the Session Initiation Protocol (SIP) is used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.
ipv4:*destination-address*	Configures the IP address of the dial peer to receive calls. The colon is required.
ipv6:[*destination-address*]	Configures the IPv6 address of the dial peer to receive calls. Square brackets must be entered around the IPv6 address. The colon is required.
dns:[$s$] *hostname*	Configures the host device housing the domain name system (DNS) server that resolves the name of the dial peer to receive calls. The colon is required. Use one of the following macros with this keyword when defining the session target for VoIP peers: • **$s$.**—(Optional) Source destination pattern is used as part of the domain name. • **$d$.**—(Optional) Destination number is used as part of the domain name. • **$e$.**—(Optional) Digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. • **$u$.**—(Optional) Unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name. • *hostname*—String that contains the complete hostname to be associated with the target address; for example, serverA.example1.com.

enum:*table-num*	Configures ENUM search table number. Range is from 1 to 15. The colon is required.
loopback:rtp	Configures all voice data to loop back to the source. The colon is required.
ras	Configures the registration, admission, and status (RAS) signaling function protocol. A gatekeeper is consulted to translate the E.164 address into an IP address.
sip-server	Configures the global SIP server is the destination for calls from the dial peer.
:*port*	(Optional) Port number for the dial-peer address. The colon is required.
settlement *provider-number*	Configures the settlement server as the target to resolve the terminating gateway address. • The *provider-number* argument specifies the provider IP address.
registrar	Specifies to route the call to the registrar end point. • The **registrar** keyword is available only for SIP dial peers.

Command Default

No IP address or domain name is defined.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was modified. This command was implemented on the Cisco AS5300. The **ras** keyword was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **settlement** and **sip-server** keywords were added.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **enum** keyword was added.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.1(3)T	This command was modified. The **registrar** keyword was added.

Usage Guidelines

Use the **session target** command to specify a network-specific destination for a dial peer to receive calls from the current dial peer. You can select an option to define a network-specific address or domain name as a target, or you can select one of several methods to automatically determine the destination for calls from the current dial peer.

Use the **session target dns** command with or without the specified macros. Using the optional macros can reduce the number of VoIP dial-peer session targets that you must configure if you have groups of numbers associated with a particular router.

The **session target enum** command instructs the dial peer to use a table of translation rules to convert the dialed number identification service (DNIS) number into a number in E.164 format. This translated number is sent to a DNS server that contains a collection of URLs. These URLs identify each user as a destination for a call and may represent various access services, such as SIP, H.323, telephone, fax, e-mail, instant messaging, and personal web pages. Before assigning the session target to the dial peer, configure an ENUM match table with the translation rules using the **voice enum-match-table** command in global configuration mode. The table is identified in the **session target enum** command with the *table-num* argument.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin.

Use the **session target dhcp** command to specify that the session target host is obtained via DHCP. The **dhcp** option can be made available only if the SIP is being used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command.

For the **session target settlement** *provider-number* command, when the VoIP dial peers are configured for a settlement server, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Use the **session target sip-server** command to name the global SIP server interface as the destination for calls from the dial peer. You must first define the SIP server interface by using the **sip-server** command in SIP user-agent (UA) configuration mode. Then you can enter the **session target sip-server** option for each dial peer instead of having to enter the entire IP address for the SIP server interface under each dial peer.

After the SIP endpoints are registered with the SIP registrar in the hosted unified communications (UC), you can use the **session target registrar** command to route the call automatically to the registrar end point. You must configure the **session target** command on a dial pointing towards the end point.

Examples

The following example shows how to create a session target using DNS for a host named “voicerouter” in the domain example.com:

```
dial-peer voice 10 voip
 session target dns:voicerouter.example.com
```

The following example shows how to create a session target using DNS with the optional **$u$**. macro. In this example, the destination pattern ends with four periods (.) to allow for any four-digit extension that has the leading number 1310555. The optional **$u$**. macro directs the gateway to use the unmatched portion of the dialed number—in this case, the four-digit extension—to identify a dial peer. The domain is “example.com.”

```
dial-peer voice 10 voip
 destination-pattern 1310555....
 session target dns:$u$.example.com
```

The following example shows how to create a session target using DNS, with the optional **$d$**. macro. In this example, the destination pattern has been configured to 13105551111. The optional macro **$d$**. directs the gateway to use the destination pattern to identify a dial peer in the “example.com” domain.

```
dial-peer voice 10 voip
 destination-pattern 13105551111
 session target dns:$d$.example.com
```

The following example shows how to create a session target using DNS, with the optional **$e$**. macro. In this example, the destination pattern has been configured to 12345. The optional macro **$e$**. directs the gateway to do the following: reverse the digits in the destination pattern, add periods between the digits, and use this reverse-exploded destination pattern to identify the dial peer in the “example.com” domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.example.com
```

The following example shows how to create a session target using an ENUM match table. It indicates that calls made using dial peer 101 should use the preferential order of rules in enum match table 3:

```
dial-peer voice 101 voip
 session target enum:3
```

The following example shows how to create a session target using DHCP:

```
dial-peer voice 1 voip
session protocol sipv2
voice-class sip outbound-proxy dhcp
session target dhcp
```

The following example shows how to create a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13105551111
 session target ras
```

The following example shows how to create a session target using settlement:

```
dial-peer voice 24 voip
 session target settlement:0
```

The following example shows how to create a session target using IPv6 for a host at 2001:10:10:10:10:10:10:230a:5090:

```
dial-peer voice 4 voip
destination-pattern 5000110011
session protocol sipv2
session target ipv6:[2001:0DB8:10:10:10:10:10:230a]:5090
codec g711ulaw
```

The following example shows how to configure Cisco Unified Border Element (UBE) to route a call to the registering end point:

```
dial-peer voice 4 voip
session target registrar
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dial-peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.
session protocol (dial peer)	Specifies a session protocol for calls between local and remote routers using the packet network dial peer configuration mode.
settle-call	Specifies that settlement is to be used for the specified dial peer, regardless of the session target type.
sip-server	Defines a network address for the SIP server interface.
voice enum-match-table	Initiates the ENUM match table definition.

sessions maximum

To set the maximum number of allowed sessions that can exist on a zone pair, use the **sessions maximum** command in parameter-map configuration mode. To change the number of allowed sessions, use the **no** form of this command.

sessions maximum *sessions*

no sessions maximum

Syntax Description

sessions	Maximum number of allowed sessions. Range: 1 to 2147483647.

Command Default

Default value is unlimited.

Command Modes

Parameter-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Use the **sessions maximum** command to limit the number of inspect sessions that match a certain class. Session limiting is activated when this parameter is configured.

This command is available only within an inspect type parameter map and takes effect only when the parameter map is associated with an inspect action in a policy.

If the **sessions maximum** command is configured, the number of established sessions on the router can be shown via the **show policy-map type inspect zone-pair** command.

Examples

The following example shows how to limit the maximum number of allowed sessions to 200 and how verify the number of established sessions:

```
parameter map type inspect abc
 sessions maximum 200

Router# show policy-map type inspect zone-pair

 Zone-pair: zp

  Service-policy inspect : test-udp

    Class-map: check-udp (match-all)
      Match: protocol udp
      Inspect
        Packet inspection statistics [process switch:fast switch]
        udp packets: [3:4454]
```

```
          Session creations since subsystem startup or last reset 92
          Current session counts (estab/half-open/terminating) [5:33:0]<---
          Maxever session counts (estab/half-open/terminating) [5:59:0]
          Last session created 00:00:06
          Last statistic reset never
          Last session creation rate 61
          Last half-open session total 33
        Police
        rate 8000 bps,1000 limit
        conformed 2327 packets, 139620 bytes; actions: transmit
        exceeded 36601 packets, 2196060 bytes; actions: drop
        conformed 6000 bps, exceed 61000 bps

      Class-map: class-default (match-any)
        Match: any
        Drop (default action)
          0 packets, 0 bytes
```

Related Commands

Command	Description
parameter map type	Creates or modifies a parameter map.

set aggressive-mode client-endpoint

To specify the Tunnel-Client-Endpoint attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode client-endpoint** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode client-endpoint *client-endpoint*

no set aggressive-mode client-endpoint *client-endpoint*

Syntax Description

client-endpoint	One of the following identification types of the initiator end of the tunnel: • ID_IPV4 (IPV4 address) • ID_FQDN (fully qualified domain name, for example "green.cisco.com") • ID_USER_FQDN (e-mail address) The ID type is translated to the corresponding ID type in Internet Key Exchange (IKE).

Command Default

The Tunnel-Client-Endpoint attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	Support for IPv6 was added.
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

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation and specify the RADIUS Tunnel-Client-Endpoint attribute, the **set aggressive-mode client-endpoint** command, along with the **set aggressive-mode password** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload.

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

set default interface

To indicate where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination, use the **set default interface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set default interface *type number* [*...type number*]

no set default interface *type number* [*...type number*]

Syntax Description

type	Interface type, used with the interface number, to which packets are output.
number	Interface number, used with the interface type, to which packets are output.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
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 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *type* and *number* arguments.

Use this command to provide certain users a different default route. If the Cisco IOS software has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the **set default interface** command that is up is used. The optionally specified interfaces are tried in turn.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which policy routing occurs. The **set** commands specify the set actions—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command with match and set route map configuration commands to define conditions for policy routing packets.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Examples

In the following example, packets that have a Level 3 length of 3 to 50 bytes and for which the software has no explicit route to the destination are output to Ethernet interface 0:

```
interface serial 0
 ip policy route-map brighton
!
route-map brighton
 match length 3 50
 set default interface ethernet 0
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in QoS policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

set dscp {*dscp-value* | *from-field* [**table** *table-map-name*]}

no set dscp {*dscp-value* | *from-field* [**table** *table-map-name*]}

Syntax Description

dscp-value	A number that sets the DSCP value. The range is from 0 to 63. The following reserved keywords can be specified instead of numeric values: • **EF** (expedited forwarding) • **AF11** (assured forwarding class AF11) • **AF12** (assured forwarding class AF12)
from-field	Specific packet-marking category to be used to set the DSCP value of the packet. Packet-marking category keywords are as follows: • **cos** • **qos-group** **Note** If you are using a table map for mapping and converting packet-marking values, this establishes the “map from” packet-marking category.
table	(Optional) Indicates that the values set in a specified table map will be used to set the DSCP value. • This keyword is used in conjunction with the *from-field* argument.
table-map-name	(Optional) Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters. • This argument is used in conjunction with the **table** keyword.

Command Default

The DSCP value in the ToS byte is not set.

Command Modes

QoS policy-map class configuration (config-pmap-c)

Command History

Release	Modification
12.2(13)T	This command was introduced. It replaced the **set ip dscp** command.
12.0(28)S	This command was modified. Support for this command in IPv6 was added on the in Cisco IOS Release 12.0(28)S
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Precedence Value and Queueing

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the "from-field" Packet-marking Category

If you are using this command as part of the Enhanced Packet Marking feature, it can specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

Note The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the **set dscp cos** command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, you must also use the **match protocol ipv6** command. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 values only, you must use the appropriate **match ip** command. Without this command, the class map may match both IPv6 and IPv4 packets, depending on the other match criteria, and the DSCP values may act upon both types of packets.

Examples

Packet-marking Values and Table Map

In the following example, the policy map called “policy1” is created to use the packet-marking values defined in a table map called “table-map1”. The table map was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the DSCP value will be set according to the CoS value defined in the table map called “table-map1”.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)# end
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, see the “Modular Quality of Service Command-Line Interface” section of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Related Commands

Command	Description
match ip dscp	Identifies one or more DSCP, AF, and CS values as a match criterion
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set precedence	Sets the precedence value in the packet header.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set extcommunity

To set Border Gateway Protocol (BGP) extended community attributes, use the **set extcommunity** command in route-map configuration mode. To delete the entry, use the **no** form of this command.

set extcommunity {**rt** [*extended-community-value*] [**additive**] | **soo** [*extended-community-value*]}

no set extcommunity

Syntax Description

rt	Specifies the route target (RT) extended community attribute.
soo	Specifies the site of origin (SOO) extended community attribute.
extended-community-value	(Optional) Specifies the value to be set. The value can be one of the following combinations: • *autonomous-system-number***:***network-number* • *ip-address***:***network-number* • *ipv6-address***:***network-number* The colon is used to separate the autonomous system number and network number, the IP address and network number, or the IPv6 address and network number. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.
additive	(Optional) Adds a route target to the existing route target list without replacing any existing route targets.

Command Default

Specifying new route targets with the **rt** keyword replaces existing route targets by default, unless the **additive** keyword is used. The use of the **additive** keyword adds the new route target to the existing route target list but does not replace any existing route targets.

Command Modes

Route-map configuration (config-route-map)

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.
12.2(33)SRB	Support for IPv6 was added.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	Support for IPv6 was added. and this command was integrated into Cisco IOS Release 12.2(33)SB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **set extcommunity** command is used to configure set clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the Provider Edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example sets the route target to extended community attribute 100:2 for routes that are permitted by the route map:

```
Router(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 2
Router(config-route-map)# set extcommunity rt 100:2
```

The following example sets the route target to extended community attribute 100:3 for routes that are permitted by the route map. The use of the **additive** keyword adds route target 100:3 to the existing route target list but does not replace any existing route targets.

```
Router(config)# access-list 3 permit 192.168.79.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 3
Router(config-route-map)# set extcommunity rt 100:3 additive
```

Note Configuring route targets with the **set extcommunity** command will replace existing route targets, unless the **additive** keyword is used.

The following example sets the site of origin to extended community attribute 100:4 for routes that are permitted by the route map:

```
Router(config)# access-list 4 permit 192.168.80.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip-address 4
Router(config-route-map)# set extcommunity soo 100:4
```

In IPv6, the following example sets the SoO to extended community attribute 100:28 for routes that are permitted by the route map:

```
(config)# router bgp 100
(config-router)# address-family ipv6 vrf red
(config-router-af)# neighbor 8008::72a route-map setsoo in
(config-router-af)# exit
(config-router)# route-map setsoo permit 10
(config-router)# set extcommnunity soo 100:28
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 65537 in asplain format, and how to set the route-target to extended community value 65537:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 65537:100
Router(config-vrf)# exit
Router(config)# route-map rt_map permit 10
Router(config-route-map)# set extcommunity rt 65537:100
Router(config-route-map)# end
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 1.1 in asdot format, and how to set the SoO to extended community attribute 1.1:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 1.1:100
Router(config-vrf)# exit
Router(config)# route-map soo_map permit 10
Router(config-route-map)# set extcommunity soo 1.1:100
Router(config-route-map)# end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
ip extcommunity-list	Creates an extended community list and controls access to it.
match extcommunity	Matches a BGP VPN extended community list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
route-target	Creates a route target extended community for a VRF.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays all route maps configured or only the one specified.

set interface

To indicate where to forward packets that pass a match clause of a route map for policy routing, use the **set interface** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set interface *type number* [*...type number*]

no set interface *type number* [*...type number*]

Syntax Description

type	Interface type, used with the interface number, to which packets are forwarded.
number	Interface number, used with the interface type, to which packets are forwarded.

Command Default

Packets that pass a match clause are not forwarded to an interface.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.3(7)T	This command was updated for use in configuring IPv6 policy-based routing (PBR).
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB, and hardware switching support was introduced for the Cisco 7600 series platform.
12.2SX	This command was integrated into 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 3.2S	This command was modified. It was integrated into Cisco IOS XE Release 3.2S.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *type* and *number* arguments.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy-routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

In PBR for IPv6, use the **ipv6 policy route-map** or **ipv6 local policy route-map** command with **match** and **set** route-map configuration commands to define conditions for policy-routing packets.

If the first interface specified with the **set interface** command is down, the optionally specified interfaces are tried in turn.

The **set** clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

A useful next hop implies an interface. As soon as a next hop and an interface are found, the packet is routed.

Specifying the **set interface null 0** command is a way to write a policy that the packet be dropped and an "unreachable" message be generated. In Cisco IOS Release 12.4(15)T and later releases, the packets are dropped; however, the "unreachable" messages are generated only when CEF is disabled.

In Cisco IOS Release 12.2(33)SRB and later releases, hardware switching support was introduced for PBR packets sent over a traffic engineering (TE) tunnel interface on a Cisco 7600 series router. When a TE tunnel interface is configured using the **set interface** command in a policy, the packets are processed in hardware. In previous releases, PBR packets sent over TE tunnels are fast switched by Route Processor software.

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are forwarded to Ethernet interface 0:

```
interface serial 0
 ip policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

In the following example for IPv6, packets with a Level 3 length of 3 to 50 bytes are forwarded to Ethernet interface 0:

```
interface serial 0
 ipv6 policy route-map testing
!
route-map testing
 match length 3 50
 set interface ethernet 0
```

In the following example, a TE tunnel interface is configured on a Cisco 7600 series router using the **set interface** command in a policy, and the packets are processed in hardware, instead of being fast switched by Route Processor software. This example can be used only with a Cisco IOS Release 12.2(33)SRB, or later release, image.

```
interface Tunnel101
 description FRR-Primary-Tunnel
 ip unnumbered Loopback0
 tunnel destination 172.17.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name p1
!
access-list 101 permit ip 10.100.0.0 0.255.255.255 any
!
route-map test permit 10
 match ip address 101
 set interface Tunnel101
!
```

```
interface GigabitEthernet9/5
 description TO_CE_C1A_FastEther-5/5
 ip address 192.168.5.1 255.255.255.0
 ip policy route-map test
 no keepalive
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ipv6 local policy route-map	Configures PBR for IPv6 for originated packets.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or enables policy routing.
set default interface	Indicates where to forward packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set ip default next-hop verify-availability	Indicates where to forward packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ip next-hop {*ip-address* [*...ip-address*] | **dynamic dhcp** | **encapsulate l3vpn** *profile name* | **peer-address** | **recursive [global** | **vrf** *vrf name*] *ip-address* | **verify-availability** [*ip-address sequence* **track** *track object number*}

no set ip next-hop *ip-address* [*...ip-address*]

Syntax Description

ip-address	IP address of the next hop to which packets are output. It must be the address of an adjacent router.
dynamic dhcp	Sets dynamically the DHCP next hop.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	The L3VPN encapsulation profile name.
peer-address	Sets the next hop to be the BGP peering address.
recursive *ip-address*	Sets the IP address of the recursive next-hop router. **Note** The next-hop IP address must be assigned separately from the recursive next-hop IP address.
global	Sets the global routing table.
vrf *vrf name*	Sets the VRF.
verify-availability	Verifies if the nexthop is reachable.
sequence	(Optional) The sequence to insert into next-hop list. The range is from 1 to 65535.
track	(Optional) Sets the next hop depending on the state of a tracked object.
track object number	(Optional) The tracked object number. The range is from 1 to 500.

Command Default

Packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.0(28)S	The **recursive** keyword was added.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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	In Cisco IOS XE Release 2.2 this command was introduced on the Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate l3vpn** keyword was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

Note The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** command causes the system to use the routing table first and then policy route the specified next hop.

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are output to the router at IP address 10.14.2.2:

```
interface serial 0
 ip policy route-map thataway
!
route-map thataway
 match length 3 50
 set ip next-hop 10.14.2.2
```

In the following example, the IP address of 10.3.3.3 is set as the recursive next-hop address:

```
route-map map_recurse
 set ip next-hop recursive 10.3.3.3
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop verify-availability	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

set ipv6 default next-hop

To specify an IPv6 default next hop to which matching packets will be forwarded, use the **set ipv6 default next-hop** command in route-map configuration mode. To delete the default next hop, use the **no** form of this command.

set ipv6 default next-hop *global-ipv6-address* [*global-ipv6-address*...]

no set ipv6 default next-hop *global-ipv6-address* [*global-ipv6-address*...]

Syntax Description

global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. 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

This command is disabled by default.

Command Modes

Route-map configuration

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

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument.

Use the **set ipv6 default next-hop** command in policy-based routing PBR for IPv6 to specify an IPv6 next-hop address to which a packet will be policy routed when the router has no route in the IPv6 routing table or the packets match the default route. The IPv6 next-hop address must be adjacent to the router; that is, reachable by using a directly connected IPv6 route in the IPv6 routing table. The IPv6 next-hop address also must be a global IPv6 address. An IPv6 link-local address cannot be used because use of an IPv6 link-local address requires interface context.

If the software has no explicit route for the destination in the packet, then it routes the packet to the next hop as specified by the **set ipv6 default next-hop** command. The optional specified IPv6 addresses are tried in turn.

Use the **ipv6 policy route-map** command, the **route-map** command, and the **match** and **set route-map** commands to define the conditions for PBR packets. The **ipv6 policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria, which are the conditions under which PBR occurs. The **set** commands specify the set actions, which are the particular routing actions to perform if the criteria enforced by the match commands are met.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Note The **set ipv6 next-hop** and **set ipv6 default next-hop** are similar commands. The **set ipv6 next-hop** command is used to policy route packets for which the router has a route in the IPv6 routing table. The **set ipv6 default next-hop** command is used to policy route packets for which the router does not have a route in the IPv6 routing table (or the packets match the default route).

Examples

The following example sets the next hop to which the packet will be routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:0678::/32 any

route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 default next-hop 2001:0089::1234
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 policy-based routing (PBR) on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 next-hop (PBR)	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 next-hop (BGP)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}

no set ipv6 next-hop {*ipv6-address* [*link-local-address*] | **encapsulate l3vpn** *profile name* | **peer-address**}

Syntax Description

ipv6-address	IPv6 global address of the next hop to which packets are output. It need not be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
link-local-address	(Optional) IPv6 link-local address of the next hop to which packets are output. It must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
profile name	Name of the Layer 3 encapsulation profile.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default

IPv6 packets are forwarded to the next hop router in the routing table.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(4)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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The **encapsulate l3vpn** keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ipv6 next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set interface**
3. **set ipv6 default next-hop**
4. **set default interface**

Examples

The following example configures the IPv6 multiprotocol BGP peer FE80::250:BFF:FE0E:A471 and sets the route map named nh6 to include the IPv6 next hop global addresses of Fast Ethernet interface 0 of the neighbor in BGP updates. The IPv6 next hop link-local address can be sent to the neighbor by the nh6 route map or from the interface specified by the **neighbor update-source** router configuration command.

```
router bgp 170
 neighbor FE80::250:BFF:FE0E:A471 remote-as 150
 neighbor FE80::250:BFF:FE0E:A471 update-source fastether 0

address-family ipv6
  neighbor FE80::250:BFF:FE0E:A471 activate
  neighbor FE80::250:BFF:FE0E:A471 route-map nh6 out

route-map nh6
 set ipv6 next-hop 3FFE:506::1
```

Note If you specify only the global IPv6 next hop address (the *ipv6-address* argument) with the **set ipv6 next-hop** command after specifying the neighbor interface (the *interface-type* argument) with the **neighbor update-source** command, the link-local address of the neighbor interface is included as the next hop in the BGP updates. Therefore, only one route map that sets the global IPv6 next hop address in BGP updates is required for multiple BGP peers that use link-local addresses.

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.

Command	Description
neighbor next-hop-self	Disables next-hop processing of BGP updates on the router.
neighbor update-source	Specifies that the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set ipv6 next-hop (PBR)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy-based routing (PBR), use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop *global-ipv6-address* [*global-ipv6-address...*]

no set ipv6 next-hop *global-ipv6-address* [*global-ipv6-address...*]

Syntax Description

global-ipv6-address	IPv6 global address of the next hop to which packets are output. The next-hop router must be an adjacent router. 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

This command is not enabled.

Command Modes

Route-map configuration

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

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *global-ipv6-address* argument. A global IPv6 address must be specified. An IPv6 link-local address cannot be used because use of an IPv6 link-local address requires interface context.

The *global-ipv6-address* argument must specify an address that is installed in the IPv6 Routing Information Base (RIB) and is directly connected. A directly connected address is an address that is covered by an IPv6 prefix configured on an interface or an address covered by an IPv6 prefix specified on a directly connected static route.

Examples

The following example sets the next hop to which the packet will be routed:

```
ipv6 access-list match-dst-1
  permit ipv6 any 2001:0678::/32 any
```

```
route-map pbr-v6-default
  match ipv6 address match-dst-1
  set ipv6 next-hop 2001:0089::1234
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set ipv6 precedence

To set the precedence value in the IPv6 packet header, use the **set ipv6 precedence** command in route-map configuration mode. To remove the precedence value, use the **no** form of this command.

set ipv6 precedence *precedence-value*

no set ipv6 precedence *precedence-value*

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.

Command Default

This command has no default behavior.

Command Modes

Route-map configuration

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

The way the network gives priority (or some type of expedited handling) to the marked traffic is through the application of weighted fair queueing (WFQ) or weighted random early detection (WRED) at points downstream in the network. Typically, you would set IPv6 precedence at the edge of the network (or administrative domain) and have queueing act on it thereafter. WFQ can speed up handling for high precedence traffic at congestion points. WRED ensures that high precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from keywords such as routine and priority to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of Cisco high-end Internet quality of service (QoS), IPv6 precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network. For example, IPv6 precedence 2 can be given 90 percent of the bandwidth on output links in the network, and IPv6 precedence 6 can be given 5 percent using the distributed weight fair queueing (DWFQ) implementation on the Versatile Interface Processors (VIPs).

Use the **route-map** global configuration command with **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set route-map** configuration commands specify the redistribution set actions to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the IPv6 precedence value to 5 for packets that pass the route map match:

```
interface serial 0
 ipv6 policy route-map texas
!
route-map cisco1
 match length 68 128
 set ipv6 precedence 5
```

Related Commands

Command	Description
ipv6 local policy route-map	Identifies a route map to use for local IPv6 PBR.
ipv6 policy route-map	Configures IPv6 PBR on an interface.
match ipv6 address	Specifies an IPv6 access list to use to match packets for PBR for IPv6.
match length	Bases policy routing on the Level 3 length of a packet.
route-map (IP)	Define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ipv6 default next-hop	Specifies an IPv6 default next hop to which matching packets will be forwarded.
set ipv6 next-hop	Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.
set ipv6 precedence	Sets the precedence value in the IPv6 packet header.

set mpls-label

To enable a route to be distributed with a Multiprotocol Label Switching (MPLS) label if the route matches the conditions specified in the route map, use the **set mpls-label** command in route-map configuration mode. To disable this function, use the **no** form of this command.

set mpls-label

no set mpls-label

Syntax Description

This command has no arguments or keywords.

Command Default

No route with an MPLS label is distributed.

Command Modes

Route-map configuration

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)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.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command can be used only with the **neighbor route-map out** command to manage outbound route maps for a Border Gateway Protocol (BGP) session.

Use the **route-map** global configuration command with **match** and **set route-map** commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to create a route map that enables the route to be distributed with a label if the IP address of the route matches an IP address in ACL1:

```
Router(config-router)# route-map incoming permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set mpls-label
```

Related Commands

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list or specifies an IPv6 access list to use to match packets for PBR for IPv6.
match mpls-label	Redistributes routes that contain MPLS labels and match the conditions specified in the route map.
neighbor route-map out	Manage outbound route maps for a BGP session.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set pfs

To optionally specify that IP security (IPsec) requests the perfect forward secrecy (PFS) Diffie-Hellman (DH) prime modulus group identifier when requesting new security associations (SAs) for a crypto map entry or when IPsec requires PFS when receiving requests for new SAs, use the **set pfs** command in crypto map configuration mode. To specify that IPsec should not request PFS during the DH exchange, use the **no** form of this command.

set pfs {**group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20**}

no set pfs

Syntax Description

group1	Specifies the 768-bit DH identifier.
group2	Specifies the 1024-bit DH identifier.
group5	Specifies the 1536-bit DH identifier.
group14	Specifies the 2048-bit DH identifier.
group15	Specifies the 3072-bit DH identifier.
group16	Specifies the 4096-bit DH identifier.
group19	Specifies the 256-bit elliptic curve DH (ECDH) identifier.
group20	Specifies the 384-bit ECDH identifier.

Defaults

By default, PFS is not requested. If no group is specified with this command, the **group1** keyword is used as the default.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
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.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 2.2	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.
12.4(22)T	Support for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers was integrated into Cisco IOS Release 12.4(22)T.
15.1(2)T	This command was modified. DH groups 19 and 20 were added in Cisco IOS Release 15.1(2)T.

Usage Guidelines

This command is available for **ipsec-isakmp** crypto map entries and dynamic crypto map entries for both IKEv1 and IKEv2.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. The default (**group1**) is sent if the **set pfs** statement does not specify a group. If the peer initiates the negotiation and the local configuration specifies PFS, the remote peer must perform a PFS exchange or the negotiation will fail. If the local configuration does not specify a group, a default of **group1** will be assumed, and an offer of either **group1** or **group2** will be accepted. If the local configuration specifies **group2**, that group *must* be part of the offer of the peer or the negotiation will fail. If the local configuration does not specify PFS, it will accept any offer of PFS from the peer.

PFS adds another level of security; if one key is ever cracked by an attacker, then only the data sent with that key will be compromised. Without PFS, data sent with other keys could be compromised also.

With PFS, every time a new security association is negotiated, a new DH exchange occurs. (This exchange requires additional processing time.)

The 1024-bit DH prime modulus group, **group2**, provides more security than **group1** but requires more processing time than **group1**.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. While there is some disagreement regarding how many bits are necessary in the DH group to protect a specific key size, it is generally agreed that **group14** is good protection for 128-bit keys, **group15** is good protection for 192-bit keys, and **group16** is good protection for 256-bit keys.

Note **group5** may be used for 128-bit keys, but **group14** is better.

The ISAKMP group and the IPsec 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 specifies that PFS should be used whenever a new security association is negotiated for the crypto map mymap 10:

```
crypto map mymap 10 ipsec-isakmp
 set pfs group2
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.

Command	Description
set security-association level per-host	Specifies that separate IPsec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

Supported Platforms Other Than Cisco 10000 Series Routers

set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

no set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

Cisco 10000 Series Routers

set precedence *precedence-value*

no set precedence *precedence-value*

Syntax Description

precedence-value	A number from 0 to 7 that sets the precedence bit in the packet header.
from-field	Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the “map from” packet-marking category. Packet-marking category keywords are as follows: • **cos** • **qos-group**
table	(Optional) Indicates that the values set in a specified table map will be used to set the precedence value.
table-map-name	(Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters.

Command Default

This command is disabled.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **set ip precedence** command.
12.0(28)S	Support for this command in IPv6 was added in Cisco IOS Release 12.0(28)S on the Cisco 12000 series Internet routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Command Compatibility

If a router is loaded with an image from this version (that is, Cisco IOS Release 12.2(13)T) that contained an old configuration, the **set ip precedence** command is still recognized. However, the **set precedence** command will be used in place of the **set ip precedence** command.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can be one value or the other, but not both.

Bit Settings

Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The **set precedence** command cannot be used with the **set dscp** command to mark the *same* packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value. The “from-field” packet-marking categories are as follows:

- CoS
- QoS group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-nam*e argument, the default action will be to copy the value associated with the “from-field” category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set precedence qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

Precedence Values in IPv6 Environments

When this command is used in IPv6 environments it can set the value in both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class-map containing this function.

Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class-map that classified packets for this action. Without the **match protocol ipv6** command, the class-map may classify both IPv6 and IPv4 packets, (depending on other match criteria) and the **set precedence** command will act upon both types of packets.

Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp** command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class-map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence** or **set dscp** command may act upon both types of packets.

Examples

In the following example, the policy map named policy-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the precedence value will be set according to the CoS value defined in table-map1.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence cos table table-map1
Router(config-pmap-c)# end
```

The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Related Commands

Command	Description
match dscp	Identifies a specific IP DSCP value as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
set dscp	Marks a packet by setting the Layer 3 DSCP value in the ToS byte.
set qos-group	Sets a group ID that can be used later to classify packets.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

Command	Description
show table-map	Displays the configuration of a specified table map or all table maps.
table-map (**value mapping**)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations, use the **set security-association lifetime** command in crypto map configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

set security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes* | **kilobytes disable**}

no set security-association lifetime {**seconds** | **kilobytes** | **kilobytes disable**}

Syntax Description

seconds *seconds*	Specifies the number of seconds a security association will live before expiring.
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires.
kilobytes disable	Disables the IPsec security association (SA) rekey based on the traffic-volume lifetime (in kilobytes). If the **no** form is used with these keywords, lifetime settings return to the default settings.

Command Default

The crypto map's security associations are negotiated according to the global lifetimes.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.3 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.
12.4(20)T	Support for IPv6 was added.
12.2(33)SXI	The **disable** keyword was added. **Note** This keyword addition is for only Cisco IOS Release 12.2(33)SXI.
15.0(1)M	The **disable** keyword was added.

Usage Guidelines

This command is available only for **ipsec-isakmp** crypto map entries and dynamic crypto map entries.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its crypto map lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations.

When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The session keys or security association expires after the first of these lifetimes is reached.

Note IPsec SA rekey can be triggered either by a timed lifetime or by a traffic-volume lifetime. To control rekey, it is recommended that you use the timed lifetime rather than the traffic-volume lifetime. When a small traffic-volume lifetime is used for IPsec SA, it causes frequent IPsec SA rekeys. High throughput of encryption or decryption traffic can cause intermittent packet drops. The minimum traffic-volume lifetime threshold of 2560 kilobytes is *not* recommended on IPsec SAs that protect a medium-to-high throughput data link because this setting can cause packet drops during rekey.

If you change a lifetime, the change will not be applied to existing security associations, but will be used in subsequent negotiations to establish security associations for data flows supported by this crypto map entry. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more detail.

To change the timed lifetime, use the **set security-association lifetime seconds** form of the command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

To change the traffic-volume lifetime, use the **set security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the key and security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security association's key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes need more CPU processing time.

The lifetime values are ignored for manually established security associations (security associations installed via an **ipsec-manual** crypto map entry).

How The Lifetimes Work

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations it will specify its global lifetime values in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of either the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the **seconds** time out or after the **kilobytes** amount of traffic is passed.

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The **seconds** lifetime and the **kilobytes** lifetime each have a jitter mechanism to avoid security association rekey collisions. The new security association is negotiated either (30 plus a random number of) seconds before the **seconds** lifetime expires or when the traffic volume reaches (90 minus a random number of) percent of the **kilobytes** lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPsec sees another packet that should be protected.

Disabling the Traffic-Volume Lifetime

The **set security-association lifetime kilobytes disable** form of the command disables the traffic-volume lifetime. Disabling the traffic-volume lifetime affects only the router on which IPsec SA rekey based on traffic-volume lifetime is configured. It does not affect the peer router's behavior or the current router's IPsec SA time-based (seconds) rekey. The **set security-association lifetime kilobytes disable** form of the command is useful when the IPsec SAs are protecting a high bandwidth data link (10-gigabit Ethernet). This option can be used to reduce packet loss in high traffic environments and to prevent frequent rekeys that are triggered by reaching the volume lifetimes.

Note The traffic-volume lifetime can also be disabled by entering the **crypto ipsec security-association lifetime kilobytes disable** command.

Examples

The following example shortens the timed lifetime for a particular crypto map entry, because there is a higher risk that the keys could be compromised for security associations belonging to the crypto map entry. The traffic-volume lifetime is not changed because there is not a high volume of traffic anticipated for these security associations. The timed lifetime is shortened to 2700 seconds (45 minutes).

```
crypto map mymap 10 ipsec-isakmp
 set security-association lifetime seconds 2700
```

The following example shows that the **kilobytes disable** keyword has been used to disable the volume lifetime.

```
set security-association lifetime kilobytes disable
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPsec security associations.
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new security associations for this crypto map entry, or that IPsec requires PFS when receiving requests for new security associations.
set security-association level per-host	Specifies that separate IPsec security associations should be requested for each source/destination host pair.

Command	Description
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set** command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

set transform-set *transform-set-name* [*transform-set-name2...transform-set-name6*]

no set transform-set

Syntax Description

transform-set-name	Name of the transform set. For an **ipsec-manual** crypto map entry, you can specify only one transform set. For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Command Default

No transform sets are included by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	Support for IPv6 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command is required for all static and dynamic crypto map entries.

Use this command to specify which transform sets to include in a crypto map entry.

For an **ipsec-isakmp** crypto map entry, you can list multiple transform sets with this command. List the higher priority transform sets first.

If the local router initiates the negotiation, the transform sets are presented to the peer in the order specified in the crypto map entry. If the peer initiates the negotiation, the local router accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec will not establish a security association. The traffic will be dropped because there is no security association to protect the traffic.

For an **ipsec-manual** crypto map entry, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

If you want to change the list of transform sets, re-specify the new list of transform sets to replace the old list. This change is only applied to crypto map entries that reference this transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

Any transform sets included in a crypto map must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example defines two transform sets and specifies that they can both be used within a crypto map entry. (This example applies only when IKE is used to establish security associations. With crypto maps used for manually established security associations, only one transform set can be included in a given crypto map entry.)

```
crypto ipsec transform-set my_t_set1 esp-des esp-sha-hmac
crypto ipsec transform-set my_t_set2 ah-sha-hmac esp-des esp-sha-hmac

crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.1
 set peer 10.0.0.2
```

In this example, when traffic matches access list 101, the security association can use either transform set "my_t_set1" (first priority) or "my_t_set2" (second priority) depending on which transform set matches the remote peer's transform sets.

set vrf

To enable VPN routing and forwarding (VRF) instance selection within a route map for policy-based routing (PBR) VRF selection, use the **set vrf** command in route-map configuration mode. To disable VRF selection within a route map, use the **no** form of this command.

set vrf *vrf-name*

no set vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to the VRF.

Command Default

VRF instance selection is not enabled within a route map for policy-based routing VRF selection.

Command Modes

Route-map configuration (config-route-map)

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(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SXI4	This command was modified. Support for IPv6 was added.

Usage Guidelines

The **set vrf** route-map configuration command was introduced with the Multi-VRF Selection Using Policy-Based Routing feature to provide a PBR mechanism for VRF selection. This command enables VRF selection by policy routing packets through a route map. The route map is attached to the incoming interface. The match criteria are defined in an IP access list or in an IP prefix list. The match criteria can also be defined based on the packet length with the **match length** route map command. The VRF must be defined before you configure this command, and the **ip policy route-map** interface configuration command must be configured to enable policy routing under the interface or subinterface. If the VRF is not defined or if policy routing is not enabled, an error message will be displayed on the console when you attempt to configure the **set vrf** command.

Note The **set vrf** command is not supported in hardware with the IP Services feature set. If this command is configured in IP Services, the packets are software switched. Hardware forwarding with this command in place requires packet circulation and is only supported in the Advanced IP Services feature set, which supports Multiprotocol Label Switching (MPLS).

In Cisco IOS Release 12.2(33)SXI4 on the Cisco Catalyst 6500, IPv6 PBR allows users to override normal destination IPv6 address-based routing and forwarding results. VRF allows multiple routing instances in Cisco IOS software. The PBR feature is VRF-aware, meaning that it works under multiple routing instances, beyond the default or global routing table.

In PBR, the **set vrf** command decouples the VRF and interface association and allows the selection of a VRF based on the ACL-based classification using the existing PBR or route-map configurations. It provides a single router with multiple routing tables and the ability to select routes based on the ACL classification. The router classifies packets based on ACL, selects a routing table, looks up the destination address, and then routes the packet.

Note The functionality provided by the **set vrf** and **set ip global next-hop** commands can also be configured with the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. However, the **set vrf** and **set ip global next-hop** commands take precedence over the **set default interface**, **set interface**, **set ip default next-hop**, and **set ip next-hop** commands. No error message is displayed indicating that VRF is already enabled if you attempt to configure the **set vrf** command with any of these four **set** commands.

Examples

The following example shows a route-map sequence that selects and sets a VRF based on the match criteria defined in three different access lists. (The access list configuration is not shown in this example.) If the route map falls through and a match does not occur, the packet will be dropped if the destination is local.

```
route-map PBR-VRF-Selection permit 10
match ip address 40
set vrf VRF1
!
route-map PBR-VRF-Selection permit 20
match ip address 50
set vrf VRF2
!
route-map PBR-VRF-Selection permit 30
match ip address 60
set vrf VRF3
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
debug ip policy	Displays the IP policy routing packet activity.
ip policy route-map	Identifies a route map to use for policy routing on an interface.
ip vrf	Configures a VRF routing table.
ip vrf receive	Inserts the IP address of an interface as a connected route entry in a VRF routing table.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

Command	Description
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.
set interface	Indicates where to forward packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.

show access-lists

To display the contents of current access lists, use the **show access-lists** command in user EXEC or privileged EXEC mode.

show access-lists [*access-list-number* | *access-list-name*]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
access-list-name	(Optional) Name of the IP access list to display.

Defaults

The system displays all access lists.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)S	The output was modified to identify the compiled ACLs.
12.1(1)E	This command was implemented on the Cisco 7200 series.
12.1(5)T	The command output was modified to identify compiled ACLs.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(2)T	The command output was modified to show information for IPv6 access lists.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.

Usage Guidelines

The **show access-lists** command is used to display the current ACLs operating in the router. Each access list is flagged using the Compiled indication if it is operating as an accelerated ACL.

The display also shows how many packets have been matched against each entry in the ACLs, enabling the user to monitor the particular packets that have been permitted or denied. This command also indicates whether the access list is running as a compiled access list.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101

Extended IP access list 101
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the **show access-lists** command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

Note The permit and deny information displayed by the **show access-lists** command may not be in the same order as that entered using the **access-list** command.

```
Router# show access-lists

Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists

IPv6 access list list2
     deny ipv6 FEC0:0:0:2::/64 any sequence 10
     permit ipv6 any any sequence 20
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

show access-list template

To display information about access control lists (ACLs), use the **show access-list template** command in privileged EXEC mode.

show access-list template {**summary** | *aclname* | **exceed** *number* | **tree**}

Syntax Description

summary	Displays summary information about ACLs.
aclname	Displays information about the specified ACL.
exceed *number*	Limits the results to template ACLs that replace more than the specified *number* of individual ACLs.
tree	Provides an easily readable summary of the frequency of use of each of the ACL types that the template ACL function sees.

Command Modes

Privileged EXEC#

Command History

Cisco IOS Release	Description
12.2(27)SBKA	This command was introduced on the Cisco 10000 series router.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

This section provides examples of the different forms of the **show access-list template** command.

show access-list template summary

The following example shows output from the **show access-list template summary** command:

```
Router# show access-list template summary

Maximum rules per template ACL = 100
Templates active = 1
Number of ACLs those templates represent = 50
Number of tree elements = 1
```

Output from this command includes:

- Maximum number of rules per template ACL
- Number of discovered active templates
- Number of ACLs replaced by those templates

show access-list template *aclname*

The following example shows output from the **show access-list template** *aclname* command:

```
Router# show access-list template 4Temp_1073741891108

    Showing data for 4Temp_1073741891108
    4Temp_1073741891108 peer_ip used is 172.17.2.62,
    is a parent, attached acl count = 98
    currentCRC = 59DAB725


Router# show access-list template 4Temp_1342177340101

    Showing data for 4Temp_1342177340101
    4Temp_1342177340101 idb's ip peer = 172.17.2.55,
    parent is 4Temp_1073741891108, user account attached to parent = 98
    currentCRC = 59DAB725
```

Output from this display includes:

- Peer IP of the interface associated with the named template ACL
- Name of the ACL serving as the primary user of the named template ACL
- Number of ACLs matching the template of the named template ACL
- Current cyclic redundancy check 32-bit (CRC32) value

show access-list template exceed *number*

The following example shows output from the **show access-list template exceed** *number* command:

```
Router# show access-list template exceed 49
ACL name                          OrigCRC    Count     CalcCRC
4Temp_#120795960097               104FB543   50      104FB543
```

Table 50 describes the significant fields shown in the display.

Table 50 show access-list template exceed Field Descriptions

Field	Description
ACL Name	Name of the template ACL. Only template ACLs that contain more than the specified number (**exceed** *number*) of child ACLs are listed.
OrigCRC	Original CRC32 value
Count	Count of ACLs that match the template ACL
CalcCRC	Calculated CRC32 value

show access-list template tree

The following example shows output from the **show access-list template tree** command:

```
Router# show access-list template tree

ACL name               OrigCRC    Count   CalcCRC
4Temp_1073741891108    59DAB725   98      59DAB725
```

Table 51 describes the significant fields shown in the display.

Table 51 show access-list template tree Field Descriptions

Field	Description
ACL name	Name of an ACL on the Red-Black tree
OrigCRC	Original CRC32 value
Count	Number of users of the ACL
CalcCRC	Calculated CRC32 value

show adjacency

To display information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table, use the **show adjacency** command in user EXEC or privileged EXEC mode.

show adjacency [*ip-address*] [*interface-type interface-number* | **null** *number* | **port-channel** *number* | **sysclock** *number* | **vlan** *number* | *ipv6-address* | **fcpa** *number* | **serial** *number*] [**connectionid** *number*] [**link** {**ipv4** | **ipv6** | **mpls**}] [**detail** | **encapsulation**]

show adjacency summary [i*nterface-type interface-number*]

Syntax Description

ip-address	(Optional) An IP address or IPv6 address. **Note** On the Cisco 10000 series routers IPv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.
interface-type interface-number	(Optional) Interface type and number. Valid values for the *interface-type* argument are **atm**, **async**, **auto-template**, **ctunnel, dialer**, **esconphy**, **fastethernet**, **filter**, **filtergroup**, **gigabitethernet**, **group-async**, **longreachethernet**, **loopback**, **mfr**, **multilink**, **portgroup**, **pos**, **tunnel**, **vif**, **virutal-template**, **voabypassin**, **voabypassout**, **voafilterin**, **voafilterout**, **voain**, and **voaout**. **Note** Not all interface types and numbers are available on all platforms. Enter the **show adjacency** command to verify the interface types for your platform.
null *number*	(Optional) Specifies the null interface. The valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are 1 to 282.
sysclock *number*	(Optional) Telecom-bus clock controller; valid values are 1 to 6.
vlan *number*	(Optional) Specifies the VLAN; valid values are 1 to 4094.
ipv6-address	(Optional) Specifies the associated IPv6 address.
fcpa *number*	(Optional) The fiber channel; valid values are 1 to 6.
serial *number*	(Optional) Specifies the serial interface number; valid values are 1 to 6.
connectionid *number*	(Optional) Specifies the client connection identification number.
link {**ipv4** | **ipv6** | **mpls**}	(Optional) Specifies the link type (IP, IPv6, or Multiprotocol Label Switching (MPLS) traffic of the adjacency).
detail	(Optional) Displays the protocol detail and timer information.
summary	(Optional) Displays a summary of Cisco Express Forwarding adjacency information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2GS	This command was introduced.
11.1CC	Multiple platform support was added.
12.0(7)XE	Support was added for the Cisco 7600 series routers.
12.1(5c)EX	This command was modified to include Layer 3 information.
12.1(11b)E	The **atm**, **ge-wan**, and **pos** keywords were added.
12.2(8)T	The **detail** keyword output was modified to show the epoch value for each entry of the adjacency table. The **summary** keyword output was modified to show the table epoch for the adjacency table.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S . The **link ipv4**, **link ipv6**, and **link mpls** keywords and the *prefix* argument were added.
12.2(28)SB	Support for IPv6 was added for the Cisco 10000 series routers.
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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **show adjacency** command is used to verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.

For line cards, you must specify the line card if_number (interface number). Use the **show cef interface** command to obtain line card if_numbers.

You can use any combination of the *ip-address, interface-type*, and other keywords and arguments (in any order) as a filter to display a specific subset of adjacencies.

On Cisco 7600 series routers, hardware Layer 3-switching adjacency statistics are updated every 60 seconds.

Note On the Cisco 10000 series routers, Pv6 is supported on Cisco IOS Release 12.2(28)SB or later releases.

The following information may be displayed by the **show adjacency** commands:

- Protocol
- Interface
- Type of routing protocol that is configured on the interface
- Type of routed protocol traffic using this adjacency
- Next hop address
- Method of adjacency that was learned
- Adjacency source (for example, Address Resolution Protocol (ARP) or ATM Map)

- Encapsulation prepended to packet switched through this adjacency
- Chain of output chain elements applied to packets after an adjacency
- Packet and byte counts
- High availability (HA) epoch and summary event epoch
- MAC address of the adjacent router
- Time left before the adjacency rolls out of the adjacency table. After the adjacency rolls out, a packet must use the same next hop to the destination.

Examples

The following examples show how to display adjacency information:

Cisco 7500 Series Router

```
Router# show adjacency

Protocol Interface                 Address
IP       FastEthernet2/3           172.20.52.1(3045)
IP       FastEthernet2/3           172.20.52.22(11)
```

The following example shows how to display adjacency information for a specific interface:

```
Router# show adjacency fastethernet 0/0

Protocol Interface                 Address
IP       FastEthernet0/0           10.4.9.2(5)
IP       FastEthernet0/0           10.4.9.3(5)
```

Cisco 10000 Series Router

```
Router# show adjacency

Protocol Interface                 Address
IP       FastEthernet2/0/0         172.20.52.1(3045)
IP       FastEthernet2/0/0         172.20.52.22(11)
```

Cisco 7500 and 10000 Series Router

The following example shows how to display detailed adjacency information for adjacent IPv6 routers:

```
Router# show adjacency detail

Protocol Interface                 Address
IP       Tunnel0                   point2point(6)
                                    0 packets, 0 bytes
                                    00000000
                                    CEF   expires: 00:02:57
                                          refresh: 00:00:57
                                    Epoch: 0
IPV6     Tunnel0                   point2point(6)
                                    0 packets, 0 bytes
                                    00000000
                                    IPv6 CEF   never
                                    Epoch: 0
IPV6     Ethernet2/0               FE80::A8BB:CCFF:FE01:9002(3)
                                    0 packets, 0 bytes
                                    AABBCC019002AABBCC012C0286DD
                                    IPv6 ND    never
                                    Epoch: 0
IPV6     Ethernet2/0               3FFE:2002::A8BB:CCFF:FE01:9002(5)
                                    0 packets, 0 bytes
                                    AABBCC019002AABBCC012C0286DD
                                    IPv6 ND    never
                                    Epoch: 0
```

Table 52 describes the significant fields shown in the displays.

Table 52 show adjacency Field Descriptions

Field	Description
Protocol	Type of Internet protocol.
Interface	Outgoing interface.
Address	Next hop IP address.

The following example shows how to display a summary of adjacency information:

```
Router# show adjacency summary

Adjacency table has 7 adjacencies:
  each adjacency consumes 368 bytes (4 bytes platform extension)
  6 complete adjacencies
  1 incomplete adjacency
  4 adjacencies of linktype IP
    4 complete adjacencies of linktype IP
    0 incomplete adjacencies of linktype IP
    0 adjacencies with fixups of linktype IP
    2 adjacencies with IP redirect of linktype IP
  3 adjacencies of linktype IPV6
    2 complete adjacencies of linktype IPV6
    1 incomplete adjacency of linktype IPV6

Adjacency database high availability:
  Database epoch: 8 (7 entries at this epoch)

Adjacency manager summary event processing:
 Summary events epoch is 52
 Summary events queue contains 0 events (high water mark 113 events)
 Summary events queue can contain 49151 events
 Adj last sourced field refreshed every 16384 summary events
RP adjacency component enabled
```

The following examples show how to display protocol detail and timer information:

For a Cisco 7500 Series Router

```
Router# show adjacency detail

Protocol Interface                 Address
IP       FastEthernet0/0           10.4.9.2(5)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 2
                                   Encap length 14
                                   00307131ABFC000500509C080800
                                   ARP
IP       FastEthernet0/0           10.4.9.3(5)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 2
                                   Encap length 14
                                   000500506C08000500509C080800
                                   ARP
```

For a Cisco 7600 Series Router

```
Router# show adjacency detail

Protocol Interface                 Address
IP       FastEthernet2/3           172.20.52.1(3045)
                                   0 packets, 0 bytes
                                   000000000FF920000380000000000000
                                   00000000000000000000000000000000
                                   00605C865B2800D0BB0F980B0800
                                   ARP        03:58:12
IP       FastEthernet2/3           172.20.52.22(11)
                                   0 packets, 0 bytes
                                   000000000FF920000380000000000000
                                   00000000000000000000000000000000
                                   00801C93804000D0BB0F980B0800
                                   ARP        03:58:06
```

For a Cisco 10000 Series Router

```
Router# show adjacency detail

Protocol Interface                 Address
IP       FastEthernet2/0/0           10.4.9.2(5)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 2
                                   Encap length 14
                                   00307131ABFC000500509C080800
                                   ARP
IP       FastEthernet2/0/0           10.4.9.3(5)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 2
                                   Encap length 14
                                   000500506C08000500509C080800
                                   ARP
```

The following examples show how to display protocol detail and timer adjacency information for IP links for a specific interface:

For a Cisco 7500 Series Router

```
Router# show adjacency tunnel 1 link detail

Protocol Interface                 Address
IP       Tunnel1                   point2point(7)
                                   0 packets, 0 bytes
                                   epoch 1
                                   sourced in sev-epoch 4
                                   empty encap string
                                   P2P-ADJ
                                   Next chain element:
                                    label 16 TAG adj out of Ethernet1/0, addr 10.0.0.0
```

For a Cisco 7600 Series Router

```
Router# show adjacency fastethernet 2/3

Protocol Interface                 Address
IP       FastEthernet2/3           172.20.52.1(3045)
IP       FastEthernet2/3           172.20.52.22(11)
```

For a Cisco 10000 Series Router

```
Router# show adjacency tunnel 1 link detail

Protocol Interface               Address
IP       Tunnel1                 point2point(7)
                                 0 packets, 0 bytes
                                 epoch 1
                                 sourced in sev-epoch 4
                                 empty encap string
                                 P2P-ADJ
                                 Next chain element:
                                 label 16 TAG adj out of FastEthernet0/0, addr 10.0.0.0
```

Related Commands

Command	Description
clear adjacency	Clears the Cisco Express Forwarding adjacency table.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
show adjacency	Enables the display of information about the adjacency database.
show mls cef adjacency	Displays information about the hardware Layer 3-switching adjacency node.
show cef interface	Displays detailed Cisco Express Forwarding information for all interfaces.

show atm map

To display the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps, use the **show atm map** command in user EXEC or privileged EXEC mode.

show atm map

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.1CA	This command was modified to include an example for the ATM-CES port adapter (PA).
12.0(3)T	This command was modified to include display for ATM bundle maps. An ATM bundle map identifies a bundle and all of its related virtual circuits (VCs).
12.2(2)T	The display output for this command was modified to include the IPv6 address mappings of remote nodes to ATM permanent virtual circuits (PVCs).
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.

Examples

The following is sample output from the **show atm map** command for a bundle called san-jose (0/122, 0/123, 0/124, and 0/126 are the virtual path and virtual channel identifiers of the bundle members):

```
Router# show atm map

Map list san-jose_B_ATM1/0.52 : PERMANENT
ip 10.1.1.1. maps to bundle san-jose, 0/122, 0/123, 0/124, 0/126, ATM1/0.52, broadcast
```

The following is sample output from the **show atm map** command for an ATM-CES PA on the Cisco 7200 series router:

```
Router# show atm map

Map list alien: PERMANENT
ip 10.1.1.1 maps to VC 6
ip 10.1.1.2 maps to VC 6
```

The following is sample output from the **show atm map** command that displays information for a bundle called new-york:

```
Router# show atm map

Map list atm:
vines 3004B310:0001 maps to VC 4, broadcast
ip 172.21.168.110 maps to VC 1, broadcast
clns 47.0004.0001.0000.0c00.6e26.00 maps to VC 6, broadcast
appletalk 10.1 maps to VC 7, broadcast
decnet 10.1 maps to VC 2, broadcast
Map list new-york: PERMANENT
ip 10.0.0.2 maps to bundle new-york, 0/200, 0/205, 0/210, ATM1/0.1
```

The following is sample output from the **show atm map** command for a multipoint connection:

```
Router# show atm map

Map list atm_pri: PERMANENT
ip 10.4.4.4 maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12, broadcast,
aal5mux, multipoint connection up, VC 6
ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12, broadcast,
aal5mux, connection up, VC 15, multipoint connection up, VC 6

Map list atm_ipx: PERMANENT
ipx 1004.dddd.dddd.dddd maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 8
ipx 1004.cccc.cccc.cccc maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 8

Map list atm_apple: PERMANENT
appletalk 62000.5 maps to NSAP CD.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 4
appletalk 62000.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12,
broadcast, aal5mux, multipoint connection up, VC 4
```

The following is sample output from the **show atm map** command if you configure an ATM PVC using the **pvc** command:

```
Router# show atm map

Map list endA: PERMANENT
ip 10.11.11.1 maps to VC 4, VPI 0, VCI 60, ATM0.2
```

The following sample output from the **show atm map** command shows the link-local and global IPv6 addresses (FE80::60:3E47:AC8:C and 2001:0DB8:2222::72, respectively) of a remote node that are explicitly mapped to PVC 1/32 of ATM interface 0;

```
Router# show atm map

Map list ATM0pvc1 : PERMANENT
ipv6 FE80::60:3E47:AC8:C maps to VC 1, VPI 1, VCI 32, ATM0
        , broadcast
ipv6 2001:0DB8:2222::72 maps to VC 1, VPI 1, VCI 32, ATM0
```

Table 53 describes the significant fields shown in the displays.

Table 53 show atm map Field Descriptions

Field	Description
Map list	Name of map list.
PERMANENT	This map entry was entered from configuration; it was not entered automatically by a process.
ip 172.21.168.110 maps to VC 1 or ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12	Name of protocol, the protocol address, and the virtual circuit descriptor (VCD) or network service access point (NSAP) to which the address is mapped (for ATM VCs configured with the **atm pvc** command).
broadcast	Indicates pseudobroadcasting.
ip 10.11.11.1 maps to VC 4, VPI 0, VCI 60, ATM0.2 or ip 10.4.4.6 maps to NSAP DE.CDEF.01.234567.890A.BCDE.F012.3456.7890.1234.12	Name of protocol, the protocol address, the virtual path identifier (VPI) number, the virtual channel identifier (VCI) number, and the ATM interface or subinterface (for ATM PVCs configured using the **pvc** command). or Name of the protocol, the protocol address, and the NSAP to which the address is mapped (for ATM switched virtual circuits (SVCs) configured using the **svc** command).
aal5mux	Indicates the encapsulation used, a multipoint or point-to-point VC, and the number of the virtual circuit.
multipoint connection up	Indicates that this is a multipoint VC.
VC 6	Number of the VC.
connection up	Indicates a point-to-point VC.
VPI	VPI for the VC.
VCI	VCI for the VC.
ATM1/0.52	ATM interface or subinterface number.
Map list	Name of the bundle whose mapping information follows.
ip 10.1.1.1 maps to bundle san-jose, 0/122, 0/123, 0/124, 0/126	IP address of the bundle and VC members that belong to the bundle.

Related Commands

Command	Description
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).
protocol ipv6 (ATM)	Maps the IPv6 address of a remote node to the ATM PVC used to reach the address.

Command	Description
pvc	Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, or enters interface-ATM-VC configuration mode.
show atm bundle	Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members.
show atm bundle statistics	Displays statistics on the specified bundle.
svc	Creates an ATM SVC and specifies destination NSAP address on an interface or subinterface.

show bfd neighbors

To display a line-by-line listing of existing Bidirectional Forwarding Detection (BFD) adjacencies, use the **show bfd neighbors** command in user EXEC or privileged EXEC mode.

show bfd neighbors [**client** {**bgp** | **eigrp** | **isis** | **ospf** | **rsvp** | **te-frr**} | **details** | [*interface-type interface-number*] | **internal** | **ipv4** *ip-address* | **ipv6** *ipv6-address* | **vrf** *vrf-name*]

Syntax Description

client	(Optional) Displays the neighbors of a specific client.
bgp	(Optional) Specifies a Border Gateway Protocol (BGP) client.
eigrp	(Optional) Specifies an Enhanced Interior Gateway Routing Protocol (EIGRP) client.
isis	(Optional) Specifies an Intermediate System-to-Intermediate System (IS-IS) client.
ospf	(Optional) Specifies an Open Shortest Path First (OSPF) client.
rsvp	(Optional) Specifies a Resource Reservation Protocol (RSVP) client.
te-frr	(Optional) Specifies a Traffic Engineering (TE) Fast Reroute (FRR) client.
details	(Optional) Displays all BFD protocol parameters and timers for each neighbor.
interface-type interface-number	(Optional) Neighbors at a specified interface.
internal	(Optional) Displays internal BFD information.
ipv4	(Optional) Specifies an IPv4 neighbor. If the **ipv4** keyword is used without the *ip-address* argument, all IPv4 sessions are displayed.
ip-address	(Optional) IP address of a neighbor in A.B.C.D format.
ipv6	(Optional) Specifies an IPv6 neighbor. If the **ipv6** keyword is used without the *ipv6-address* argument, all IPv6 sessions are displayed.
ipv6-address	(Optional) IPv6 address of a neighbor in X:X:X:X::X format.
vrf *vrf-name*	(Optional) Displays entries for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

S Release	Modification
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **vrf** *vrf-name* keyword and argument, the **client** keyword, and the *ip-address* argument were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was modified. The output was modified to display the “OurAddr” field only with the **details** keyword.

12.2(33)SRE	This command was modified. Support for IPv6 was added.
15.1(2)S	This command was modified. • The **show bfd neighbors details** command output was changed for hardware-offloaded BFD sessions. • The **show bfd neighbors** command output was changed to show the header type identifying the session type.
T Release	**Modification**
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(9)T	This command was modified. Support for BFD Version 1 and BFD echo mode was added.
15.1(2)T	This command was modified. Support for IPv6 was added.
X Release	**Modification**
Cisco IOS XE Release 2.1	This command was modified. Support for IPv6 was added.

Usage Guidelines

The **show bfd neighbors** command can be used to help troubleshoot the BFD feature.

The full output for the **details** keyword is not supported on the Route Processor (RP) for the Cisco 12000 series Internet router. If you want to enter the **show bfd neighbors** command with the **details** keyword on the Cisco 12000 series Internet router, you must enter the command on the line card. Use the **attach** *slot* command to establish a CLI session with a line card.

In Cisco IOS Release 15.1(2)S and later releases that support BFD hardware offload, the Tx and Rx intervals on both BFD peers must be configured in multiples of 50 milliseconds. If they are not, output from the **show bfd neighbors details** command will show the configured intervals, not the changed ones.

See the "Configuring Synchronous Ethernet on the Cisco 7600 Router with ES+ Line Card" section of the *Cisco 7600 Series Ethernet Services Plus (ES+) and Ethernet Services Plus T (ES+T) Line Card Configuration Guide* for more information about prerequisites and restrictions for hardware offload.

Examples

Examples for Cisco IOS Release 12.0(31)S, 12.2(18)SXE, 12.2(33)SRA, 12.2(33)SB, and 12.4(4)T

The following sample output shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors

OurAddr       NeighAddr      LD/RD RH  Holdown(mult) State     Int
172.16.10.1   172.16.10.2    1/6  1   260  (3 )      Up        Fa0/1
```

The following sample output from the **show bfd neighbors** command entered with the **details** keyword shows BFD protocol parameters and timers for each neighbor:

```
Router# show bfd neighbors details

NeighAddr                         LD/RD    RH/RS     State     Int
10.1.1.2                           1/1         1(RH) Up        Et0/0
Session state is UP and not using echo function.
OurAddr: 10.1.1.1
Local Diag: 0, Demand mode: 0, Poll bit: 0
```

```
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3 Received MinRxInt: 50000, Received
Multiplier: 3 Holddown (hits): 150(0), Hello (hits): 50(2223) Rx Count: 2212, Rx Interval
(ms) min/max/avg: 8/68/49 last: 0 ms ago Tx Count: 2222, Tx Interval (ms) min/max/avg:
40/60/49 last: 20 ms ago Elapsed time watermarks: 0 0 (last: 0) Registered protocols: CEF
Stub
Uptime: 00:01:49
Last packet: Version: 0                  - Diagnostic: 0
             I Hear You bit: 1           - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 1                - Your Discr.: 1
             Min tx interval: 50000      - Min rx interval: 50000
             Min Echo interval: 50000
```

The following sample output from the RP on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor:

```
Router# show bfd neighbors

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0  0   0    (0 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from the RP on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# show bfd neighbors details

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/0  0   0    (0 )      Up        Fa6/0
Registered protocols: OSPF
Uptime: never
%% BFD Neighbor statistics are not available on RP. Please execute this command on Line
Card.
```

The following sample output from a line card on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor:

```
Router# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session

Press RETURN to get started!

Router> show bfd neighbors

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1  1   848  (5 )      Up        Fa6/0
 Total Adjs Found: 1
```

The following sample output from a line card on a Cisco 12000 series Internet router shows the status of the adjacency or neighbor with the **details** keyword:

```
Router# attach 6

Entering Console for 8 Port Fast Ethernet in Slot: 6
Type "exit" to end this session
```

```
Press RETURN to get started!

Router> show bfd neighbors details

Cleanup timer hits: 0

OurAddr       NeighAddr     LD/RD RH  Holdown(mult)  State     Int
172.16.10.2   172.16.10.1    2/1  1   892  (5 )      Up        Fa6/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 1000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 1000(0), Hello (hits): 200(193745)
Rx Count: 327406, Rx Interval (ms) min/max/avg: 152/248/196 last: 108 ms ago
Tx Count: 193748, Tx Interval (ms) min/max/avg: 204/440/331 last: 408 ms ago
Last packet: Version: 0            - Diagnostic: 0
             I Hear You bit: 1     - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 5         - Length: 24
             My Discr.: 1          - Your Discr.: 2
             Min tx interval: 200000    - Min rx interval: 200000
             Min Echo interval: 0
Uptime: 17:54:07
SSO Cleanup Timer called: 0
SSO Cleanup Action Taken: 0
Pseudo pre-emptive process count: 7728507 min/max/avg: 8/16/8 last: 12 ms ago
 IPC Tx Failure Count: 0
 IPC Rx Failure Count: 0
 Total Adjs Found: 1
LC-Slot6>
```

Example for 12.4(9)T and Later Releases

The following sample output verifies that the BFD neighbor router is also running BFD Version 1 and that the BFD session is up and running in echo mode:

```
Router# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
172.16.1.2    172.16.1.1     1/6    Up        0    (3 )   Up        Fa0/1
Session state is UP and using echo function with 50 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000    - Min rx interval: 1000000
             Min Echo interval: 50000
```

Example for Cisco IOS XE Release 2.1 and Later Releases

The following example displays all IPv6 sessions:

```
Router# show bfd neighbors ipv6 2001::1

OurAddr    NeighAddr  LD/RD  RH/RS  Holddown(mult)  State  Int
1:1::5     1:1::6      2/2    Up        0    (3 )   Up     Et0/0
```

```
2:2::5     2:2::6      4/4    Up        0    (3 )   Up     Et1/0
```

Examples for Cisco IOS Release 12.2(33)SXI, 12.2(33)SRE, 12.2(33)XNA, and Later Releases

The following is sample output from the **show bfd neighbors** command:

```
Router# show bfd neighbors

NeighAddr                         LD/RD    RH/RS     State     Int
192.0.2.1                          4/0     Down      Down      Et0/0
192.0.2.2                          5/0     Down      Down      Et0/0
192.0.2.3                          6/0     Down      Down      Et0/0
192.0.2.4                          7/0     Down      Down      Et0/0
192.0.2.5                          8/0     Down      Down      Et0/0
192.0.2.6                         11/0         0(RH) Fail      Et0/0
1000:1:1:1:1:1:1:2                 9/0     Down      Down      Et0/0
1000:1:1:1:1:1:1:810              10/0     Down      Down      Et0/0
1000:1111:1111:111:11:111:11:5     1/0         0(RH) Fail      Et0/0
1000:1111:1111:111:11:111:11:6     2/0     Down      Down      Et0/0
1000:1111:1111:1111:1111:1111:1111:8810
                                   3/0     Down      Down      Et0/0
```

The following is sample output from the **show bfd neighbors details** command:

```
Router# show bfd neighbors details

NeighAddr                         LD/RD    RH/RS     State     Int
192.0.2.5                          4/0     Down      Down      Et0/0
OurAddr: 192.0.2.8
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(120)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 118672 ms ago
Tx Count: 120, Tx Interval (ms) min/max/avg: 760/1000/885 last: 904 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1            - Diagnostic: 0
             State bit: AdminDown  - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 0         - Length: 0
             My Discr.: 0          - Your Discr.: 0
             Min tx interval: 0    - Min rx interval: 0
             Min Echo interval: 0


NeighAddr                         LD/RD    RH/RS     State     Int
1000:1:1:1:1:1:1:2                 9/0     Down      Down      Et0/0
OurAddr: 1000:1:1:1:1:1:1:1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holddown (hits): 0(0), Hello (hits): 1000(208)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 194760 ms ago
Tx Count: 208, Tx Interval (ms) min/max/avg: 760/1000/878 last: 424 ms ago
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: Stub
Last packet: Version: 1            - Diagnostic: 0
             State bit: AdminDown  - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 0         - Length: 0
             My Discr.: 0          - Your Discr.: 0
             Min tx interval: 0    - Min rx interval: 0
```

```
          Min Echo interval: 0
```

Table 54 describes the significant fields shown in the displays.

Table 54 show bfd neighbors Field Descriptions

Field	Description
OurAddr	IP address of the interface for which the **show bfd neighbors details** command was entered.
NeighAddr	IPv4 or IPv6 address of the BFD adjacency or neighbor.
LD/RD	Local discriminator and remote discriminator being used for the session.
RH	Remote Heard—Indicates that the remote BFD neighbor has been heard.
Holdown(mult)	The detect timer multiplier that is used for this session.
State	State of the interface—Up or Down.
Int	Interface type and slot/port.
Session state is UP and using echo function with 50 ms interval.	BFD is up and running in echo mode. The 50-millisecond interval has been adopted from the **bfd** command. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Rx Count	Number of BFD control packets that have been received from the BFD neighbor.
Tx Count	Number of BFD control packets that have been sent by the BFD neighbor.
Tx Interval	The interval, in milliseconds, between sent BFD packets.
Registered protocols	Routing protocols that have been registered with BFD.
Last packet: Version:	BFD version detected and run between the BFD neighbors. The system automatically performs BFD version detection, and BFD sessions between neighbors will run in the highest common BFD version between neighbors. For example, if one BFD neighbor is running BFD Version 0, and the other BFD neighbor is running Version 1, the session will run BFD Version 0. **Note** BFD Version 1 and echo mode are supported only with Cisco IOS Release 12.4(9)T and later releases.
Diagnostic	A diagnostic code specifying the local system's reason for the last transition of the session from Up to some other state. State values are as follows: • 0—No Diagnostic • 1—Control Detection Time Expired • 2—Echo Function Failed • 3—Neighbor Signaled Session Down • 4—Forwarding Plane Reset • 5—Path Down • 6—Concentrated Path Down • 7—Administratively Down

Table 54 show bfd neighbors Field Descriptions (continued)

Field	Description
I Hear You bit	The I Hear You Bit is set to 0 if the transmitting system is either not receiving BFD packets from the remote system or is tearing down the BFD session for some reason. During normal operation, the I Hear You bit is set to 1 to signify that the remote system is receiving the BFD packets from the transmitting system.
Demand bit	Demand Mode bit. BFD has two modes—asynchronous and demand. If the Demand Mode is set, the transmitting system prefers to operate in demand mode. The Cisco implementation of BFD supports only asynchronous mode.
Poll bit	If the Poll bit is set, the transmitting system is requesting verification of connectivity or verification of a parameter change.
Final bit	If the Final bit is set, the transmitting system is responding to a received BFD control packet that had a Poll (P) bit set.
Multiplier	Detect time multiplier. The negotiated transmit interval multiplied by the detect time multiplier determines the detection time for the transmitting system in BFD asynchronous mode. The detect time multiplier is similar to the hello multiplier in Intermediate System-to-Intermediate System (IS-IS), which is used to determine the hold timer: (hello interval) * (hello multiplier) = hold timer. If a hello packet is not received within the hold-timer interval, a failure has occurred. Similarly, for BFD: (transmit interval) * (detect multiplier) = detect timer. If a BFD control packet is not received from the remote system within the detect-timer interval, a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discr.	My Discriminator. Unique, nonzero discriminator value generated by the transmitting system used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discr.	Your Discriminator. The discriminator received from the corresponding remote system. This field reflects the received value of My Discriminator, or is zero if that value is unknown.
Min tx interval	Minimum transmission interval, in microseconds, that the local system wants to use when sending BFD control packets.
Min rx interval	Minimum receipt interval, in microseconds, between received BFD control packets that the system can support.
Min Echo interval	Minimum interval, in microseconds, between received BFD control packets that the system can support. If the value is zero, the transmitting system does not support the receipt of BFD echo packets. The Cisco implementation of BFD for Cisco IOS Releases 12.2(18)SXE and 12.0(31)S does not support the use of echo packets.

Example for Cisco IOS Release 15.1(2)S with Hardware Offload to Cisco 7600 Series Routers

The following is sample output from the **show bfd neighbors details** command for BFD sessions offloaded to hardware. The Rx and Tx counts show the number of packets received and transmitted by the BFD session in hardware.

```
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.1                              298/298        Up        Up        Te7/1.2
Session state is UP and not using echo function.
Session Host: Hardware - session negotiated with platform adjusted timer values.
              Holddown - negotiated: 510000      adjusted: 0
OurAddr: 192.0.2.2
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 170000, MinRxInt: 170000, Multiplier: 3
Received MinRxInt: 160000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 170(0)
Rx Count: 1256983
Tx Count: 24990
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: OSPF CEF
Uptime: 18:11:31
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             Multiplier: 3               - Length: 24
             My Discr.: 298                 - Your Discr.: 298
             Min tx interval: 160000     - Min rx interval: 160000
             Min Echo interval: 0
```

Examples for Cisco IOS Release 15.1(2)S with Changes in the Header Line in the Output

The following is sample output from the **show bfd neighbors** command showing a header type identifying the type of session:

```
Router# show bfd neighbors

MPLS-TP Sessions
Interface       LSP type                  LD/RD    RH/RS     State
Tunnel-tp1      Working                    1/0     Down      Down
Tunnel-tp2      Working                    3/0     Down      Down
Tunnel-tp1      Protect                    2/0     Down      Down


IPv4 Sessions
NeighAddr                         LD/RD    RH/RS     State     Int
192.0.2.1                           2/0     Down      Down      Et2/0
```

The following is sample output from the **show bfd neighbors** command for Virtual Circuit Connection Verification (VCCV) sessions:

```
Router# show bfd neighbors

VCCV Sessions
Peer Addr      :VCID                     LD/RD    RH/RS     State
198.51.100.1   :100                       1/1     Up        Up
```

The following is sample output from the **show bfd neighbors** command for IPv4 and IPv6 sessions:

```
Router# show bfd neighbors

IPv4 Sessions
NeighAddr                            LD/RD    RH/RS     State     Int
192.0.2.1                             6/0     Down      Down      Et1/0
203.0.113.1                           7/6     Up        Up        Et3/0
198.51.100.2                          8/7     Up        Up        Et0/0

IPv6 Sessions
NeighAddr                         LD/RD    RH/RS     State     Int
CC::2                              1/1     Up        Up        Et0/0
```

```
DD::2                                  2/2     Up         Up         Et0/0
EE::2                                  3/3     Up         Up         Et0/0
ABCD::2                                4/4     Up         Up         Et0/0
FE80::2                                5/5     Up         Up         Et0/0
```

Table 55 describes the significant fields shown in the displays.

Table 55 show bfd neighbors Field Descriptions

Field	Description
Interface	Name of the MPLS tunnel TP interface.
LSP type	Type of label switched path for this session (Working or Protect).

Related Commands

Command	Description
attach	Connects to a specific line card to execute monitoring and maintenance commands on that line card.

show bfd summary

To display summary information for Bidirectional Forwarding Protocol (BFD), use the **show bfd summary** command in user EXEC or privileged EXEC mode.

show bfd summary [**client** | **session**]

Syntax Description

client	(Optional) Displays list of BFD clients and number of sessions created by each client.
session	(Optional) Displays list of client-to-peer exchanges that have been launched by BFD clients, organized by session type.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use this command to display summary information about BFD, BFD clients, or BFD sessions.

When a BFD client launches a session with a peer, BFD sends periodic BFD control packets to the peer. Information about the following states of a session are included in the output of this command:

- Up—When another BFD interface acknowledges the BFD control packets, the session moves into an up state.
- Down—The session, and data path, is declared down if a data path failure occurs and BFD does not receive a control packet within the configured amount of time. When a session is down, BFD notifies the BFD client so that the client can perform necessary actions to reroute traffic.

Examples

The following is sample output from the **show bfd summary** command:

```
Router# show bfd summary

                    Session          Up          Down

Total                     1           1             0
```

The following is sample output from the **show bfd summary session** command:

```
Router# show bfd summary session

Protocol            Session          Up          Down
IPV4                      1           1             0

Total                     1           1             0
```

The following is sample output from the **show bfd summary client** command:

```
Router# show bfd summary client
```

```
Client                Session         Up           Down
EIGRP                       1          1              0
CEF                         1          1              0

Total                       2          2              0
```

Table 56 describes the significant fields shown in the display.

Table 56 show bfd summary Field Descriptions

Field	Description
Session	Sum of launched sessions by type or when combined with Total, sum of all launched sessions.
Up	Number of sessions for which the BFD client acknowleged receipt of control packets.
Down	Number of sessions for which the BFD client did not receive control packets from a peer.
Total	Sum of all launched sessions, all Up sessions, or all Down sessions in list.
Protocol	Routing protocol of interface in a session.
Client	Type of client in a session.

Related Commands

Command	Description
show bfd neighbors	Displays list of existing BFD adjacencies.

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the **show bgp ipv6** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
ipv6-prefix	(Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays the route and more specific routes.
labels	(Optional) Displays Multiprotocol Label Switching (MPLS) label information.

Command Modes

User EXEC
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	MPLS label information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	MPLS label value advertised for the IPv6 prefix was added to the display.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.2(25)S	6PE multipath information was added to the display.
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 **show bgp ipv6** command provides output similar to the **show ip bgp** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6** command:

```
Router# show bgp ipv6 unicast

BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                        0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                           0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1             0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                           0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                           0 3320 1275 559 i
*                   3FFE:C00:E:9::2                        0 1251 1930 559 i
*                   3FFE:3600::A                           0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                           0 293 1275 559 i
*                   3FFE:C00:E:4::2          1             0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                        0 237 3748 1275 559 i
```

Table 57 describes the significant fields shown in the display.

Table 57 show bgp ipv6 Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.

Table 57 show bgp ipv6 Field Descriptions (continued)

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6** command, showing information for prefix 3FFE:500::/24:

```
Router# show bgp ipv6 unicast 3FFE:500::/24

BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  Advertised to peer-groups:
     6BONE
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 673, flapped 429 times in 10:47:45
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 3938, flapped 596 times in 13:03:06, reuse in 00:59:10
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
```

The following is sample output from the **show bgp ipv6** command, showing MPLS label information for an IPv6 prefix that is configured to be an IPv6 edge router using MPLS:

```
Router# show bgp ipv6 unicast 2001:0DB8::/32

BGP routing table entry for 2001:0DB8::/32, version 15
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best, mpls label 17
```

To display the top of the stack label with label switching information, enter the **show bgp ipv6** EXEC command with the **labels** keyword:

```
Router# show bgp ipv6 unicast labels

Network              Next Hop               In tag/Out tag
2001:0DB8::/32       ::FFFF:192.168.99.70   notag/20
```

Note If a prefix has not been advertised to any peer, the display shows "Not advertised to any peer."

The following is sample output from the **show bgp ipv6** command, showing 6PE multipath information. The prefix 4004::/64 is received by BGP from two different peers and therefore two different paths:

```
Router# show bgp ipv6 unicast

BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path

*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community

To display routes that belong to specified IPv6 Border Gateway Protocol (BGP) communities, use the **show bgp ipv6 community** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community** [*community-number*] [**exact-match**] [**local-as** | **no-advertise** | **no-export**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
community-number	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

Command Modes

User EXEC
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.
12.3(2)T	The **unicast** and **exact-match** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.

Usage Guidelines

The **show bgp ipv6 community** command provides output similar to the **show ip bgp community** command, except it is IPv6-specific.

Communities are set with the **set community** route-map configuration command. You must enter the numerical communities before the well-known communities. For example, the following string is not valid:

```
Router# show ipv6 bgp community local-as 111:12345
```

Use one of the following strings instead:

```
Router# show ipv6 bgp community 111:12345 local-as

Router# show ipv6 bgp unicast community 111:12345 local-as
```

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 community** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

       Network               Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                       0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                       0 32768 ?
*> 2001:0DB8:0:2::/64        2001:0DB8:0:3::2                            0 2 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:3::2                            0 2 ?
* 2001:0DB8:0:3::1/64        2001:0DB8:0:3::2                            0 2 ?
*>                        ::                                       0 32768 ?
*> 2001:0DB8:0:4::/64        2001:0DB8:0:3::2                            0 2 ?
*> 2001:0DB8:0:5::1/64       ::                                       0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                            0 2 3 i
*> 2010::/64                 ::                                       0 32768 ?
*> 2020::/64                 ::                                       0 32768 ?
*> 2030::/64                 ::                                       0 32768 ?
*> 2040::/64                 ::                                       0 32768 ?
*> 2050::/64                 ::                                       0 32768 ?
```

Table 58 describes the significant fields shown in the display.

Table 58 show bgp ipv6 community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).

Table 58 show bgp ipv6 community Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
ip bgp-community new-format	Displays BGP communities in the format AA:NN (autonomous system-community number:2-byte number).
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 community-list

To display routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list, use the **show bgp ipv6 community-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **community-list** {*number* | *name*} [**exact-match**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
number	Community list number in the range from 1 to 199.
name	Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC
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.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.

Usage Guidelines

The **show bgp ipv6 unicast community-list** and **show bgp ipv6 multicast community-list** commands provide output similar to the **show ip bgp community-list** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output of the **show bgp ipv6 community-list** command for community list number 3:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast community-list 3

BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                 Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64       2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64      ::                                    0 32768 i
*> 2001:0DB8:0:2:1::/80     ::                                    0 32768 ?
* 2001:0DB8:0:3::2/64       2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                    0 32768 ?
*> 2001:0DB8:0:4::2/64      ::                                    0 32768 ?
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                         0 1 ?
```

Table 59 describes the significant fields shown in the display.

Table 59 show bgp ipv6 community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.

Table 59 show bgp ipv6 community-list Field Descriptions (continued)

Field	Description
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp ipv6 dampened-paths

To display IPv6 Border Gateway Protocol (BGP) dampened routes, use the **show bgp ipv6 dampened-paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening dampened-paths**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.

Command Modes

User EXEC
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.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.

Usage Guidelines

The **show bgp ipv6 dampened-paths** and **show bgp ipv6 unicast dampening dampened-paths** commands provide output similar to the **show ip bgp dampened-paths** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 dampened-paths** command:

Note The command output is the same whether or not the **unicast, multicast,** and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening dampened-paths

BGP table version is 12610, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network           From              Reuse    Path
*d 3FFE:1000::/24    3FFE:C00:E:B::2   00:00:10 237 2839 5609 i
*d 2001:228::/35     3FFE:C00:E:B::2   00:23:30 237 2839 5609 2713 i
```

Table 60 describes the significant fields shown in the display.

Table 60 show bgp ipv6 dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.
Network	Indicates the network to which the route is dampened.
From	IPv6 address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 dampening	Clears IPv6 BGP route dampening information and unsuppresses the suppressed routes.

show bgp ipv6 filter-list

To display routes that conform to a specified IPv6 filter list, use the **show bgp ipv6 filter-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **filter-list** *access-list-number*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
access-list-number	Number of an IPv6 autonomous system path access list. It can be a number from 1 to 199.

Command Modes

User EXEC
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.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.

Usage Guidelines

The **show bgp ipv6 filter-list** command provides output similar to the **show ip bgp filter-list** command, except that it is IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 filter-list** command for IPv6 autonomous system path access list number 1:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast filter-list 1

BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network              Next Hop                          Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                        0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                        0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                        0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                        0 2 ?
*> 2001:0DB8:0:4::/64        ::                                        32768  ?
*                            2001:0DB8:0:4::2                        0 2 ?
*> 2001:0DB8:0:5::/64        ::                                        32768  ?
*                            2001:0DB8:0:4::2                        0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                        32768  i
*> 2030::/64                 2001:0DB8:0:4::2                        0 1
*> 2040::/64                 2001:0DB8:0:4::2                        0 2 1 ?
*> 2050::/64                 2001:0DB8:0:4::2                        0 2 1 ?
```

Table 61 describes the significant fields shown in the display.

Table 61 show bgp ipv6 filter-list Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented any time the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.

Table 61 show bgp ipv6 filter-list Field Descriptions (continued)

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i—The entry was originated with the IGP and advertised with a **network** router configuration command. • e—The route originated with EGP. • ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

Related Commands

Command	Description
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 flap-statistics

To display IPv6 Border Gateway Protocol (BGP) flap statistics, use the **show bgp ipv6 flap-statistics** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **dampening flap-statistics** [**regexp** *regular-expression* | **quote-regexp** *regular-expression* | **filter-list** *list* | *ipv6-prefix***/***prefix-length* [**longer-prefix**]]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
dampening	Displays detailed information about dampening.
regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regexp *regular-expression*	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list *list*	(Optional) Displays flap statistics for all the paths that pass the access list.
ipv6-prefix	(Optional) Displays flap statistics for a single entry at this IPv6 network number. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

User EXEC
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.
12.3(2)T	The **unicast** and **dampening** keywords were added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** 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.

Usage Guidelines

The **show bgp ipv6 unicast dampening flap-statistics** and **show bgp ipv6 multicast dampening flap-statistics** commands provide output similar to the **show ip bgp flap-statistics** command, except they are IPv6-specific.

If no arguments or keywords are specified, the router displays flap statistics for all routes.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 flap-statistics** command without arguments or keywords:

Note The output is the same whether or not the **unicast, multicast,** and **dampening** keywords are used. The **unicast** and **dampening** keywords are available only in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast dampening flap-statistics

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          From            Flaps Duration Reuse    Path
*d 2001:200::/35    3FFE:1100:0:CC00::1
                                    12145 10:09:15 00:57:10 1849 2914 4697 2500
*  2001:218::/35    2001:0DB8:0:F004::1
                                    2     00:03:44          3462 4697
```

Table 62 describes the significant fields shown in the display.

Table 62 show bgp ipv6 flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).

Table 62 show bgp ipv6 flap-statistics Field Descriptions (continued)

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IPv6 address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp ipv6 flap-statistics	Clears IPv6 BGP flap statistics.
ip as-path access-list	Defines a BGP autonomous system path access list.

show bgp ipv6 inconsistent-as

To display IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems, use the **show bgp ipv6 inconsistent-as** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **inconsistent-as**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
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.
12.3(2)T	The **unicast** keyword was added.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **multicast** keyword was 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.

Usage Guidelines

The **show bgp ipv6 unicast inconsistent-as** and **show bgp ipv6 multicast inconsistent-as** commands provide output similar to the **show ip bgp inconsistent-as** command, except they are IPv6-specific.

The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and later releases. It is not available in releases prior to 12.3(2)T. Use of the **unicast** keyword is mandatory starting with Cisco IOS Release 12.3(2)T.

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 inconsistent-as** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast inconsistent-as

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                        0 1251 4270 10318 ?
*                   3FFE:3600::A                           0 3462 6175 ?
*                   3FFE:700:20:1::11                      0 293 6175 ?
```

Table 63 describes the significant fields shown in the display.

Table 63 show bgp ipv6 inconsistent-as Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from the Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	The value of the interautonomous system metric. This field is frequently not used.

Table 63 show bgp ipv6 inconsistent-as Field Descriptions (continued)

Field	Description
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp ipv6 labels

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 labels** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast** | **multicast**} **labels**

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.0(26)S	The **unicast** and **multicast** keywords were added.
12.3(4)T	The **unicast** and **multicast** keywords were added.

Usage Guidelines

The **multicast** keyword is available in Cisco IOS Release 12.0(26)S and later releases. It is not available in releases prior to 12.0(26)S. Use of either the **unicast** or **multicast** keyword is mandatory starting with Cisco IOS Release 12.0(26)S.

Examples

The following is sample output from the **show bgp ipv6 labels** command:

Note The output is the same whether or not the **unicast** or **multicast** keyword is used. The **unicast** keyword is available in Cisco IOS Release 12.3(2)T and Cisco IOS Release 12.0(26)S and later releases, and the **multicast** keyword is available only in Cisco IOS Release 12.0(26)S and later releases.

```
Router# show bgp ipv6 unicast labels

Network                     Next Hop        In label/Out label
2001:1:101::1/128           ::FFFF:172.17.1.1  nolabel/19
2001:3:101::1/128           ::FFFF:172.25.8.8  nolabel/19
```

Table 64 describes the significant fields shown in the display.

Table 64 show bgp ipv6 labels Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.

Table 64 show bgp ipv6 labels Field Descriptions (continued)

Field	Description
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
In label/Out label	IPv6 BGP connections.