snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the **snmp-server user** command in global configuration mode. To remove a user from an SNMP group, use the **no** form of this command.

snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]

no snmp-server user *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** |**256**}} *privpassword*] {*acl-number* | *acl-name*}]

Syntax Description

username	Name of the user on the host that connects to the agent.
group-name	Name of the group to which the user belongs.
remote	(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.
host	(Optional) Name or IP address of the remote SNMP host.
udp-port	(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.
port	(Optional) Integer value that identifies the UDP port. The default is 162.
vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
v1	Specifies that SNMPv1 should be used.
v2c	Specifies that SNMPv2c should be used.
v3	Specifies that the SNMPv3 security model should be used. Allows the use of the **encrypted** keyword or **auth** keyword or both.
encrypted	(Optional) Specifies whether the password appears in encrypted format.
auth	(Optional) Specifies which authentication level should be used.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
auth-password	(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.
access	(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.
ipv6	(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.
nacl	(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.
priv	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.

des	(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.
128	(Optional) Specifies the use of a 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of a 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of a 256-bit AES algorithm for encryption.
privpassword	(Optional) String (not to exceed 64 characters) that specifies the privacy user password.
acl-number	(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.
acl-name	(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.

Command Default

See Table 327 in the "Usage Guidelines" section for default behaviors for encryption, passwords, and access lists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.3(2)T	Support for named standard access lists was added.
12.0(27)S	The **ipv6** keyword and *nacl* argument were added to allow for configuration of IPv6 named access lists and IPv6 remote hosts.
12.3(14)T	The **ipv6** keyword and *nacl* argument were 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.
12.4(11)T	The **priv** keyword and associated arguments were added to enable the use of the USM for SNMP version 3 for SNMP message level security.
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 Aggregation Services Routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** command with the **remote** keyword. The remote agent's SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the *privpassword* and *auth-password* arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers.

Table 327 describes the default user characteristics for encryption, passwords, and access lists.

Table 327 snmp-server user Default Descriptions

Characteristic	Default
Access lists	Access from all IP access lists is permitted.
Encryption	Not present by default. The **encrypted** keyword is used to specify that the passwords are message digest algorithm 5 (MD5) digests and not text passwords.
Passwords	Assumed to be text strings.
Remote users	All users are assumed to be local to this SNMP engine unless you specify they are remote with the **remote** keyword.

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent's SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Note Changing the engine ID after configuring the SNMP user, does not allow to remove the user. To remove the user, you need to first reconfigure the SNMP user.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the SNMP server group named public. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

```
Router(config)# snmp-server user abcd public v2c
```

The following example shows how to add the user abcd to the SNMP server group named public. In this example, access rules from the standard named access list qrst apply to the user.

```
Router(config)# snmp-server user abcd public v2c access qrst
```

In the following example, the plain-text password cisco123 is configured for the user abcd in the SNMP server group named public:

```
Router(config)# snmp-server user abcd public v3 auth md5 cisco123
```

When you enter a **show running-config** command, a line for this user will be displayed. To learn if this user has been added to the configuration, use the **show snmp user** command.

Note The **show running-config** command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the **show snmp user** command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain-text password:

```
Router(config)# snmp-server user abcd public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

In the following example, the user abcd is removed from the SNMP server group named public:

```
Router(config)# no snmp-server user abcd public v2c
```

In the following example, the user abcd from the SNMP server group named public specifies the use of the 168-bit 3DES algorithm for privacy encryption with secure3des as the password.

```
Router(config)# snmp-server user abcd public priv v2c 3des secure3des
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.
show snmp user	Displays information on each SNMP username in the group username table.
snmp-server engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]

no snmp trap link-status [permit duplicates]

Syntax Description.

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface configuration (config-if)
Service instance configuration (config-if-srv)

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	The **permit duplicates** keyword pair was added in Cisco IOS Release 12.2(30)S.
12.3(8)T	Support for the **permit duplicates** keyword pair was integrated in Cisco IOS Release 12.3(8)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode in Cisco IOS Release 12.2(33)SRD1.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces expected to go up and down during normal usage, such as ISDN interfaces, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

By default, in service instance configuration mode SNMP link traps are not sent. Also, the **permit duplicates** keyword pair is not available in service instance configuration mode.

Cisco 10000 Series Router Usage Guidelines

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the router no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI 0 interface:

```
Router(config)# interface bri 0
Router(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Router(config)# interface ethernet 0/1
Router(config-if)# service instance 50 ethernet
Router(config-if-srv)# snmp trap link-status
Router(config-if-srv)# exit
```

Related Commands

Command	Description
virtual-template snmp	Allows virtual access interfaces to register with SNMP when they are created or reused.

sntp address

To specify the IPv6 Simple Network Time Protocol (SNTP) server address list to be sent to the client, use the **sntp address** command in DHCP for IPv6 pool configuration mode. To remove the SNTP server address list, use the **no** form of the command.

sntp address *ipv6-address*

no sntp address *ipv6-address*

Syntax Description

ipv6-address	The IPv6 SNTP address of a server to be sent to the client.

Command Default

No SNTP server address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The SNTP server address list option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers.

Clients must treat the list of SNTP servers as an ordered list, and the server may list the SNTP servers in decreasing order of preference. The option defined in this document can be used only to configure information about SNTP servers that can be reached using IPv6.

The SNTP server option code is 31. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.2.

Examples

The following example shows how to specify the SNTP server address:

```
sntp address 300::1
```

Related Commands

Command	Description
import sntp address	Imports the SNTP server option to a DHCP for IPv6 client.

spd extended-headroom

To configure Selective Packet Discard (SPD) extended headroom, use the **spd extended-headroom** command in global configuration mode. To return to the default value, use the **no** form of this command.

spd extended-headroom *size*

no spd extended-headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD extended headroom default is 10 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Because Interior Gateway Protocols (IGPs) and link stability are tenuous and crucial, such packets are given the highest priority and are given extended SPD headroom with a default of 10 packets. These packets are not dropped if the size of the input hold queue is lower than 185 (input queue default size + SPD headroom size + SPD extended headroom).

Examples

The following example shows how to configure SPD extended headroom to be 11 packets:

```
Router(config)# spd extended-headroom 11
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd headroom	Configures SPD headroom.

spd headroom

To configure Selective Packet Discard (SPD) headroom, use the **spd headroom** command in global configuration mode. To return to the default value, use the **no** form of this command.

spd headroom *size*

no spd headroom

Syntax Description

size	SPD headroom size, in number of packets.

Command Default

The SPD headroom default is 100 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

SPD prioritizes IPv6 packets with a precedence of 7 by allowing the software to queue them into the process level input queue above the normal input queue limit. The number of packets allowed in excess of the normal limit is called the SPD headroom, the default being 100, which means that a high precedence packet is not dropped if the size of the input hold queue is lower than 175 (input queue default size + SPD headroom size).

Examples

The following example shows how to configure SPD headroom to be 95 packets:

```
Router(config)# spd headroom 95
```

Related Commands

Command	Description
show ipv6 spd	Displays the IPv6 SPD configuration.
spd extended-headroom	Configures SPD extended headroom.

spf-interval (IPv6)

To configure how often Cisco IOS software performs the shortest path first (SPF) calculation, use the **spf-interval** command in address family configuration mode. To restore the default interval, use the **no** form of this command.

spf-interval [**level-1** | **level-2**] *seconds* [*initial-wait*] [*secondary-wait*]

no spf-interval *seconds*

Syntax Description

level-1	(Optional) Summarizes only routes redistributed into Level 1 with the configured prefix value.
level-2	(Optional) Summarizes routes learned by Level 1 routing into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS also are summarized.
seconds	Minimum amount of time between SPF calculations, in seconds. It can be a number from 1 to 120. The default is 5 seconds.
initial-wait	(Optional) Length of time before the first SPF calculation in milliseconds.
secondary-wait	(Optional) Minimum length of time between the first and second SPF calculation, in milliseconds.

Command Default

The default is 5 seconds.

Command Modes

Address family configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.6	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** (IPv6) command controls how often Cisco IOS software can perform the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often the SPF calculation is performed, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but it could slow down the rate of convergence.

If IPv6 and IPv4 are configured on the same interface, they must be running the same Intermediate System-to-Intermediate System (IS-IS) level.

You can use the **spf-interval** (IPv6) command only when using the IS-IS multitopology support for IPv6 feature.

Examples

The following example sets the SPF calculation interval to 30 seconds:

```
Router(config)# router isis
Router(config-router)# address-family ipv6
Router(config-router-af)# spf-interval 30
```

Related Commands

Command	Description
prc-interval (IPv6)	Controls the hold-down period between PRCs.

split-horizon (IPv6 RIP)

To configure split horizon processing of IPv6 Routing Information Protocol (RIP) router updates, use the **split-horizon** command in router configuration mode. To disable the split horizon processing of IPv6 RIP updates, use the **no** form of this command.

split-horizon

no split-horizon

Syntax Description

This command has no arguments or keywords.

Command Default

Split horizon is configured and active by default. However, for ATM interfaces and subinterfaces **split-horizon** is disabled by default.

Command Modes

Router configuration

Command History

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

Usage Guidelines

The **split-horizon** (IPv6 RIP) command is similar to the **ip split-horizon** command, except that it is IPv6-specific.

This command configures split horizon processing of IPv6 RIP router updates. When split horizon is configured, the advertisement of networks out the interfaces from which the networks are learned is suppressed.

If both split horizon and poison reverse are configured, then split horizon behavior is replaced by poison reverse behavior (routes learned via RIP are advertised out the interface over which they were learned, but with an unreachable metric).

Note In general, changing the state of the default for the **split-horizon** command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example configures split horizon processing for the IPv6 RIP routing process named cisco:

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# split-horizon
```

Related Commands

Command	Description
neighbor (RIP)	Defines a neighboring router with which to exchange routing information.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in privileged EXEC or user EXEC mode.

ssh [**-v** {**1** | **2**}] [**-c** {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}] [**-l** *userid* | **-l** *userid*:*vrfname number ip-address* | **-l** *userid*:**rotary***number ip-address*] [**-m** {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*] [**-vrf**]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. • **1**—Connects using SSH Version 1. • ***2***—Connects using SSH Version 2.
-c {**3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc**}	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms supported are aes128-cbc, aes192-cbc, and aes256-cbc. • To use SSH Version 1, you must have an encryption image running on the router. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES). • SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, aes256-cbc, and 3des-cbc. SSH Version 2 is supported only in 3DES images. • If you do not specify the **-c** keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the **-c** keyword and the server does not support the argument that you have shown (des, 3des, aes128-cbc, aes192-cbc, or aes256-cbc), the remote networking device closes the connection.
-l *userid*	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.

-l *userid***:***vrfname number ip-address*	(Optional) Specifies the user ID when configuring reverse SSH by including port information in the *userid* field. • **:**—Signifies that a port number and terminal IP address will follow the user ID. • *vrfname* — User specific VRF. • *number*—Terminal or auxiliary line number. • *ip-address*—IP address of the terminal server. **Note** The *userid* argument and **:***number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including port information in the *userid* field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line).The *vrfname* allows SSH to establish sessions with hosts whose addresses are in a VRF instance.
-l *userid***:rotary***number ip-address*	(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH. • **:**—Signifies that a rotary group number and terminal IP address will follow. • *number*—Terminal or auxiliary line number. • *ip-address*—IP address of the terminal server. **Note** The *userid* argument and **:rotary**{*number*} {*ip-address*} delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the *userid* field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).
-m {**hmac-md5 | hmac-md5-96 | hmac-sha1 | hmac-sha1-96**}	(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm. • SSH Version 1 does not support HMACs. • If you do not specify the **-m** keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the **-m** keyword and the server does not support the argument that you have shown (hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96), the remote device closes the connection.
-o numberofpasswordprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswordprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p *port-num*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.

ip-addr | *hostname*	Specifies the IPv4 or IPv6 address or host name of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.
-vrf	(Optional) Adds VRF awareness to SSH client side functionality. VRF instance name in the client is provided with the IP address to lookup the correct routing table and establish a connection.

Command Default

No encrypted session exists if the command is not used.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(8)T	Support for IPv6 addresses was added.
12.0(21)ST	IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.3(7)T	This command was expanded to include Secure Shell Version 2 support. The **-c** keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The **-m** keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The **-v** keyword and arguments **1** and **2** were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **-l** *userid***:***number ip-address* and **-l** *userid***:rotary***number ip-address* keyword and argument options 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.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The**-l** *userid***:***vrfname number ip-address* keyword and argument and **-vrf** keyword were added.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Note

- SSH Version 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- SSH Version 2 supports only the following crypto algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

The following example illustrates the initiation of a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates the initiation of a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for authentication to work.

```
ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local router and a remote IPv6 router with the address 3ffe:1111:2222:1044::72 to run the **show running-config** command. In this example, the remote IPv6 router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 router will return the result of the **show running-config** command to the local router and will then close the session.

```
ssh -l adminHQ 3ffe:1111:2222:1044::72 "show running-config"
```

Note A hostname that maps to the IPv6 address 3ffe:1111:2222:1044::72 could have been used in the last example.

The following example shows a SSH Version 2 session using the crypto algorithm aes256-cbc and an HMAC of hmac-sha1-96. The user ID is user2, and the IP address is 10.76.82.24.

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -1 user2 10.76.82.24
```

The following example shows that reverse SSH has been configured on the SSH client:

```
ssh -l lab:1 router.example.com
```

The following command shows that Reverse SSH will connect to the first free line in the rotary group:

```
ssh -l lab:rotary1 router.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the router.
show ip ssh	Displays the version and configuration data for SSH.
show ssh	Displays the status of SSH server connections.

standby ipv6

To activate the Hot Standby Router Protocol (HSRP) in IPv6, use the **standby ipv6** command in interface configuration mode. To disable HSRP, use the **no** form of this command.

standby [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address*/*prefix-length* | *ipv6-prefix*/*prefix-length* | *link-local-address* | **autoconfig**}

no standby [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address*/*prefix-length* | *ipv6-prefix*/*prefix-length* | *link-local-address* | **autoconfig**}

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
ipv6-global-address	IPv6 address of the hot standby router interface.
ipv6-prefix	The IPv6 network assigned to the interface. 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	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.
link-local-address	Link-local address of the hot standby router interface.
autoconfig	Indicates that a virtual link-local address will be generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

Command Default

The default group number is 0.
HSRP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI4	Users can configure a fully routable global virtual IPv6 address.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

An Ethernet or FDDI type interface must be used for HSRP for IPv6. HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

The **standby ipv6** command enables an HSRP group for IPv6 operation. If the **autoconfig** keyword is used, then a link-local address will be generated from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

If an IPv6 global address is used, it must include an IPv6 prefix length. If a link-local address is used, it does not have a prefix.

Examples

The following example enables an HSRP group for IPv6 operation:

```
Router(config)# standby version 2
Router(config)# interface ethernet 0
Router(config-if)# standby ipv6 autoconfig
```

The following example shows three HSRP global IPv6 addresses with an explicitly configured link-local address:

```
interface Ethernet0/0
 no ip address
 ipv6 address 2001::0DB8:1/64
 standby version 2
 standby 1 ipv6 FE80::1:CAFÉ
 standby 1 ipv6 2001::0DB8:2/64
 standby 1 ipv6 2001:0DB8::3/64
 standby 1 ipv6 2001:0DB8::4/64
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

no standby [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *seconds*	(Optional) Specifies the minimum delay period in seconds. The *seconds* argument causes the local router to postpone taking over the active role for a minimum number of seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
reload *seconds*	(Optional) Specifies the preemption delay, in seconds, after a reload only. This delay period applies only to the first interface-up event after the router has reloaded.
sync *seconds*	(Optional) Specifies the maximum synchronization period for IP redundancy clients in seconds.

Command Default

The default group number is 0.
The default delay is 0 seconds; if the router wants to preempt, it will do so immediately.
By default, the router that comes up later becomes the standby.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(2)T	The **minimum** and **sync** keywords were added.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.2	The **reload** keyword was added.
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.

Release	Modification
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines

Note Cisco IOS 12.2SX software releases earlier than Cisco IOS Release 12.2(33)SXH use the syntax from Cisco IOS Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Cisco IOS Release 12.2(33)SXH and later releases use Cisco IOS Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands.

When the **standby preempt** command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If preemption is not configured, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

This command is separate from the **standby delay minimum reload** interface configuration command, which delays HSRP groups from initializing for the specified time after the interface comes up.

When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it will become the active router, yet it is unable to provide adequate routing services. Solve this problem by configuring a delay before the preempting router actually preempts the currently active router.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

IP redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *seconds* command specifies a maximum number of seconds to allow IP redundancy clients to prevent preemption. When this expires, then preemption takes place regardless of the state of the IP redundancy clients.

The **standby preempt delay reload** *seconds* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command will disable the preemption delay but preemption will remain enabled. The **no standby preempt delay minimum** *seconds* command will disable the minimum delay but leave any synchronization delay if it was configured.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router will wait for 300 seconds (5 minutes) before attempting to become the active router:

```
Router(config)# interface ethernet 0
Router(config-if)# standby ip 172.19.108.254
```

```
Router(config-if)# standby preempt delay minimum 300
```

standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** command in interface configuration mode. To restore the default values, use the **no** form of this command.

standby [*group-number*] **priority** *priority*

no standby [*group-number*] **priority** *priority*

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply. The default group number is 0.
priority	Priority value that prioritizes a potential Hot Standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.

Command Default

The default group number is 0.
The default priority is 100.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.
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	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
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.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines

Note Cisco IOS 12.2SX software releases earlier than Cisco IOS Release 12.2(33)SXH use the syntax from Cisco IOS Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Cisco IOS Release 12.2(33)SXH and later releases use Cisco IOS Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands.

When group number 0 is used, the number 0 is written to NVRAM, providing backward compatibility.

The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.

Note that the priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router or a tracked object goes down.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router has a priority of 120 (higher than the default value):

```
Router(config)# interface ethernet 0
Router(config-if)# standby ip 172.19.108.254
Router(config-if)# standby priority 120
Router(config-if)# standby preempt delay 300
```

Related Commands

Command	Description
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

standby version

To change the version of the Hot Standby Router Protocol (HSRP), use the **standby version** command in interface configuration mode. To change to the default version, use the **no** form of this command.

standby version {**1** | **2**}

no standby version

Syntax Description

1	Specifies HSRP version 1.
2	Specifies HSRP version 2.

Command Default

HSRP version 1 is the default HSRP version.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

HSRP version 2 addresses limitations of HSRP version 1 by providing an expanded group number range of 0 to 4095.

HSRP version 2 does not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same router. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. You cannot change from version 2 to version 1 if you have configured groups above 255. Use the **no standby version** command to set the HSRP version to the default version, version 1.

If an HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

Examples

The following example shows how to configure HSRP version 2 on an interface with a group number of 500:

```
Router(config)# interface vlan500
Router(config-if)# standby version 2
Router(config-if)# standby 500 ip 172.20.100.10
Router(config-if)# standby 500 priority 110
Router(config-if)# standby 500 preempt
Router(config-if)# standby 500 timers 5 15
```

Related Commands

Command	Description
show standby	Displays HSRP information.

stub

Note Effective with Cisco IOS Release 15.0(1)M and 12.2(33)SRE, the **stub** command was replaced by the **eigrp stub** command. See the **eigrp stub** command for more information.

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

stub [**receive-only** | **connected** | **static** | **summary** | **redistributed**]

no stub [**receive-only** | **connected** | **static** | **summary** | **redistributed**]

Syntax Description

receive-only	(Optional) Sets the router as a receive-only neighbor.
connected	(Optional) Advertises connected routes.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.
redistributed	(Optional) Advertises redistributed routes from other protocols and autonomous systems.

Command Default

Stub routing is not enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.0(1)M	This command was replaced by the **eigrp stub** command.
12.2(33)SRE	This command was replaced by the **eigrp stub** command.

Usage Guidelines

Use the **stub** command to configure a router as a stub where the router directs all IPv6 traffic to a distribution router.

The **stub** command can be modified with keywords, and more than one keyword can be used in the same syntax. These options can be used in any combination, except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The **connected**, **static**, **summary**, and **redistributed** keywords can be used in any combination but cannot be used with the **receive-only** keyword.

If any of these four keywords is used with the **stub** command, only the route types specified by the particular keywords will be sent. Route types specified by the nonused keywords will not be sent.

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

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

The **summary** keyword permits the EIGRP stub routing feature to send summary routes. Summary routes can be created manually with the **ipv6 summary address eigrp** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

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

Note Multiaccess interfaces such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25 are supported by the EIGRP stub routing feature only when all routers on that interface, except the hub, are configured as stub routers.

Examples

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

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64
 stub
```

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

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64
 stub connected static
```

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

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64 eigrp
 stub receive-only
```

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

```
ipv6 router eigrp 1
 network 3FEE:12E1:2AC1:EA32::/64 eigrp
 stub redistributed
```

Related Commands

Command	Description
auto-summary (EIGRP)	Allows automatic summarization of subnet routes into network-level routes.
ipv6 summary-address eigrp	Configures a summary aggregate address for a specified interface.
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [*x.500-name*]

no subject-name [*x.500-name*]

Syntax Description

x.500-name	(Optional) Specifies the subject name used in the certificate request.

Defaults

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

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) was added.

Usage Guidelines

Before you can issue the **subject-name** 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.

The **subject-name** command is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Examples

The following example shows how to specify the subject name for the “frog” certificate:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokme
```

Related Commands

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

summary-prefix (IPv6 IS-IS)

To create aggregate IPv6 prefixes for Intermediate System-to-Intermediate System (IS-IS), use the **summary-prefix** command in address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *ipv6-prefix*/*prefix-length* {**level-1** | **level-1-2** | **level-2**}

no summary-prefix *ipv6-prefix*/*prefix-length* {**level-1** | **level-1-2** | **level-2**}

Syntax Description

ipv6-prefix	Summary prefix designated for a range of IPv6 prefixes. The *ipv6-prefix* 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	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.
level-1	Only routes redistributed into Level 1 are summarized with the configured prefix value.
level-1-2	Summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertises Level 1 routes reachable in its area.
level-2	Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured prefix value. Redistributed routes into Level 2 IS-IS will be summarized also.

Command Default

All redistributed routes are advertised individually.

Command Modes

Address family configuration

Command History

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

Usage Guidelines

Multiple groups of prefixes can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing updates generated by the router, resulting in smaller routing tables on neighbor routers.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps ensure stability because a summary advertisement is depending on many more specific routes. If one more specific route flaps, in most cases this flapping does not cause a flap of the summary advertisement.

The drawback of summary prefixes is that other routes might have less information with which to calculate the most optimal routing table for all individual destinations.

Note When IS-IS advertises a summary prefix, it automatically inserts the summary prefix into the IPv6 routing table but labels it as a "discard" route entry. Any packet that matches the entry will be discarded to prevent routing loops. When IS-IS stops advertising the summary prefix, the routing table entry is removed.

Examples

The following example redistributes Routing Information Protocol (RIP) routes into IS-IS. In the RIP routing table, there are IPv6 routes for 3FFE:F000:0001:0000::/64, 3FFE:F000:0002:0000::/64, 3FFE:F000:0003:0000::/64, and so on. This example advertises only 3FFE:F000::/24 into IPv6 IS-IS Level 1.

```
Router(config)# router isis area01
Router(config-router)# address-family ipv6
Router(config-router-af)# redistribute rip level-1 metric 40
Router(config-router-af)# summary-prefix 3FFE:F000::/24 level-1
```

summary-prefix (OSPFv3)

To configure an IPv6 summary prefix in Open Shortest Path First version 3 (OSPFv3), use the **summary-prefix** command in OSPFv3 router configuration mode, IPv6 address family configuration mode, or IPv4 address family configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

no summary-prefix *prefix* [**not-advertise** | **tag** *tag-value*]

Syntax Description

prefix	IPv6 route prefix for the destination.
not-advertise	(Optional) Suppress routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only.
tag *tag-value*	(Optional) Tag value that can be used as a "match" value for controlling redistribution via route maps. This keyword applies to OSPFv3 only.

Command Default

No IPv6 summary prefix is defined.

Command Modes

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

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)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.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

This command can be used to summarize routers redistributed from other routing protocols. Multiple groups of addresses can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Examples

In the following example, tthe summary prefix FEC0::/24 includes addresses FEC0::/1 through FEC0::/24. Only the address FEC0::/24 is advertised in an external link-state advertisement.

```
summary-prefix FEC0::/24
```

Related Commands

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

switchport

Cisco 3550, 4000, and 4500 Series Switches

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface into Layer 3 mode, use the **no** form of this command.

switchport

no switchport

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

To modify the switching characteristics of the Layer 2-switched interface, use the **switchport** command (without keywords). Use the **no** form of this command (without keywords) to return the interface to the routed-interface status and cause all further Layer 2 configuration to be erased. Use the **switchport** commands (with keywords) to configure the switching characteristics.

switchport

switchport {**host** | **nonegotiate**}

no switchport

no switchport nonegotiate

Syntax Description

Cisco 3550, 4000, and 4500 Series Switches

This command has no arguments or keywords.

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

host	Optimizes the port configuration for a host connection.
nonegotiate	Specifies that the device will not engage in negotiation protocol on this interface.

Defaults

Cisco 3550, 4000, and 4500 Series Switches

All interfaces are in Layer 2 mode.

Catalyst 6500/6000 Series Switches and 7600 Series Routers

The default access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)EA1	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(15)ZJ	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Cisco 3550, 4000, and 4500 Series Switches

Use the **no switchport** command to put the interface into the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port. Entering the **no switchport** command shuts down the port and then reenables it, which might generate messages on the device to which the port is connected.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter additional **switchport** commands with keywords. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

To optimize the port configuration, entering the **switchport host** command sets the switch port mode to access, enables spanning tree PortFast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning-tree PortFast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other Cisco 7600 series routers, hubs, concentrators, switches, and bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

The **no** form of the **switchport nonegotiate** command removes **nonegotiate** status.

When using the **nonegotiate** keyword, Dynamic Inter-Switch Link Protocol and Dynamic Trunking Protocol (DISL/DTP)-negotiation packets are not sent on the interface. The device trunks or does not trunk according to the **mode** parameter given: **access** or **trunk**. This command returns an error if you attempt to execute it in **dynamic** (**auto** or **desirable**) mode.

You must force a port to trunk before you can configure it as a SPAN-destination port. Use the **switchport nonegotiate** command to force the port to trunk.

Examples

Cisco 3550, 4000, and 4500 Series Switches

The following example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed (Layer 3) port:

```
Router(config-if)# no switchport
```

Cisco Catalyst 6500/6000 Series Switches and Cisco 7600 Series Routers

The following example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2-switched interface:

```
Router(config-if)# switchport
Router(config-if)#
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

The following example shows how to optimize the port configuration for a host connection:

```
Router(config-if)# switchport host

switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Router(config-if)#
```

This example shows how to cause a port interface that has already been configured as a switched interface to refrain from negotiating trunking mode and act as a trunk or access port (depending on the **mode** set):

```
Router(config-if)# switchport nonegotiate
Router(config-if)#
```

The following example shows how to cause an interface to cease operating as a Cisco-routed port and to convert it into a Layer 2 switched interface:

```
Router(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed (Layer 3) ports. All physical ports on such platforms are assumed to be Layer 2 switched interfaces.

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the current operating configuration.
switchport mode	Sets the interface type.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

switchport access vlan

To set the VLAN when the interface is in access mode, use the **switchport access vlan** command in interface configuration mode. To reset the access-mode VLAN to the appropriate default VLAN for the device, use the **no** form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

vlan-id	VLAN to set when the interface is in access mode; valid values are from 1 to 4094.

Defaults

The defaults are as follows:

- Access VLAN and trunk-interface native VLAN are default VLANs that correspond to the platform or interface hardware.
- All VLAN lists include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport access vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

Entering the **no switchport** command shuts down the port and then reenables it. This action may generate messages on the device to which the port is connected.

The **no** form of the **switchport access vlan** command resets the access-mode VLAN to the appropriate default VLAN for the device.

Examples

This example shows how to cause the port interface to stop operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Router(config-if)# switchport
```

Note The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

This example shows how to cause a port interface that has already been configured as a switched interface to operate in VLAN 2 instead of the platform's default VLAN in the interface-configuration mode:

```
Router(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport	Configures a LAN interface as a Layer 2 interface.

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. Use the appropriate **no** form of this command to reset the mode to the appropriate default mode for the device.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

switchport mode {**access** | **trunk**}

no switchport mode

Cisco Catalyst 6500/6000 Series Switches

switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}

no switchport mode

Cisco 7600 Series Routers

switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **private-vlan** | **trunk**}

no switchport mode

switchport mode private-vlan {**host** | **promiscuous**}

no switchport mode private-vlan

Syntax Description

access	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dot1q-tunnel	Sets the trunking mode to TUNNEL unconditionally.
dynamic auto	Sets the interface to convert the link to a trunk link.
dynamic desirable	Sets the interface to actively attempt to convert the link to a trunk link.
private-vlan host	Specifies that the ports with a valid private VLAN (PVLAN) association become active host private VLAN ports.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Defaults

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The default is **access** mode.

Cisco Catalyst 6500/6000 Switches

The default mode is dependent on the platform; it should be either **dynamic auto** for platforms that are intended as wiring closets or **dynamic desirable** for platforms that are intended as backbone switches. The default for PVLAN ports is that no mode is set.

Cisco 7600 Series Routers

The defaults are as follows:

- The mode is dependent on the platform; it should either be **dynamic auto** for platforms that are intended for wiring closets or **dynamic desirable** for platforms that are intended as backbone switches.
- No mode is set for PVLAN ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Cisco Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Cisco Catalyst 6000 family switches.
12.1(8a)EX	The switchport mode **private-vlan** {**host** | **promiscuous**} syntax was added.
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on 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.

Usage Guidelines

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

If you configure a port as a promiscuous or host-PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a SPAN destination.

If you delete a private-port PVLAN association or mapping, or if you configure a private port as a SPAN destination, the deleted private-port PVLAN association or mapping or the private port that is configured as a SPAN destination becomes inactive.

If you enter **dot1q-tunnel** mode, PortFast Bridge Protocol Data Unit (BPDU) filtering is enabled and Cisco Discovery Protocol (CDP) is disabled on protocol-tunneled interfaces.

Examples

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to set the interface to **access** desirable mode:

```
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router(config-if)# switchport mode trunk
```

Cisco Catalyst 6500/6000 Switches and Cisco 7600 Series Routers

The following example shows how to set the interface to dynamic desirable mode:

```
Router(config-if)# switchport mode dynamic desirable
Router(config-if)#
```

The following example shows how to set a port to PVLAN-host mode:

```
Router(config-if)# switchport mode private-vlan host
Router(config-if)#
```

The following example shows how to set a port to PVLAN-promiscuous mode:

```
Router(config-if)# switchport mode private-vlan promiscuous
Router(config-if)#
```

Related Commands

Command	Description
show dot1q-tunnel	Displays a list of 802.1Q tunnel-enabled ports.
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays trunk information.
switchport	Modifies the switching characteristics of the Layer 2-switched interface.
switchport private-vlan host-association	Defines a PVLAN association for an isolated or community port.
switchport private-vlan mapping	Defines the PVLAN mapping for a promiscuous port.
switchport trunk	Sets trunk characteristics when the interface is in trunking mode.

synchronization (IPv6)

To enable the synchronization between IPv6 Border Gateway Protocol (BGP) and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description

This command has no arguments or keywords.

Command Default

BGP advertises network routes without waiting for IGP.

Command Modes

Address family configuration

Command History

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

Usage Guidelines

Unlike the IPv4 version of the **synchronization** command, the IPv6 version is disabled by default.

By default, an IPv6 BGP speaker advertises an IPv6 network route without waiting for the IGP. Use the **synchronization** command in address family configuration mode to synchronize routing advertisements between BGP and your IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems. When synchronization is enabled, IPv6 BGP does not advertise a route to an external neighbor unless that route is local or exists in the IGP.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following example enables a router to advertise an IPv6 network route without waiting for an IGP:

```
router bgp 65000
address-family ipv6
 synchronization
```

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*

no tacacs server

Syntax Description

name	Name of the private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection (TACACS+)	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout (TACACS+)	Configures the time to wait for a reply from the specified TACACS server.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description

host	A hostname or an IP address.
port	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
keyword	(Optional) One of the keywords listed in Table 328.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **/ipv4** and **/ipv6** keywords were added.
12.1	The **/quiet** keyword was added.
12.2(2)T	The **/ipv4** and **/ipv6** keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(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)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

Table 328 lists the optional **telnet** command keywords.

Table 328 telnet Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).

Table 328 telnet Keyword Options (continued)

Option	Description
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the **Enter** key. You can edit the line using the standard Cisco IOS software command-editing characters. The **/line** keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: *path*	Specifies loose source routing. The *path* argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/stream	Turns on *stream* processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
port-number	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd *rcmd*	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.

Table 328 telnet Keyword Options (continued)

Option	Description
nntp	Network News Transport Protocol.
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname—as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. Table 329 lists the special Telnet escape sequences.

Table 329 Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)

Table 329 Special Telnet Escape Sequences

Escape Sequence[1]	Purpose
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

1. The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt:

Ctrl-^ ?

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router> telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to example.com, then to 10.1.0.11, and finally back to *host1*:

```
router> telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name host1:

```
router> host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router> telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32

Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

timeout (TACACS+)

To configure the time to wait for a reply from the specified TACACS server, use the **timeout** command in TACACS+ server configuration mode. To return to the command default, use the **no** form of this command.

timeout *seconds*

no timeout *seconds*

Syntax Description

seconds	(Optional) Amount of time, in seconds.

Command Default

Time to wait is 5 seconds.

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 **timeout** command to set the time, in seconds, to wait for a reply from the TACACS server. If the **timeout** command is configured, the specified number of seconds overrides the default time of 5 seconds.

Examples

The following example shows how to configure the wait time to 10 seconds:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

Related Commands

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

timers (IPv6 RIP)

To configure update, timeout, hold-down, and garbage-collection timers for an IPv6 RIP routing process, use the **timers** command in router configuration mode. To return the timers to their default values, use the **no** form of this command.

timers *update timeout holddown garbage-collection*

no timers

Syntax Description

update	Interval of time (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.
timeout	Interval of time (in seconds) after which a route is declared invalid; it should be at least three times the value of the *update* argument. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters a hold-down state. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.
holddown	Interval (in seconds) during which routing information regarding better paths is suppressed. A route enters a hold-down state when it becomes unreachable and the hold-down timer is a value other than zero. (A learned RIP route becomes unreachable when the route is not refreshed or the route is advertised with a metric of 16.) While in hold-down state, the system ignores any new information about the route from RIP or from any protocols that have a worse administrative distance than RIP. A route with a better administrative distance will replace the unreachable route, even if the route is still in a hold-down state.
garbage-collection	Amount of time (in seconds) that must pass from when a route becomes invalid until the route is removed from the routing table.

Command Default

Update timer: 30 seconds
Timeout timer: 180 seconds
Hold-down timer: 0 seconds
Garbage-collection timer: 120 seconds

Command Modes

Router configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S, and the hold-down timer default value was changed to 0 seconds.
12.2(13)T	The hold-down timer default value was changed to 0 seconds.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

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

Usage Guidelines

The **timers** (IPv6 RIP) command is similar to the **timers basic** (RIP) command, except that it is IPv6-specific.

Use the *update* argument to set the time interval between RIP routing updates. If no route update is received for the time interval specified by the *timeout* argument, the route is considered unreachable. Use the *holddown* argument to set a time delay between the route becoming unreachable and the route being considered invalid in the routing table. The use of a hold-down interval is not recommended for RIP because it can introduce long delays in convergence. Use the *garbage-collection* argument to specify the time interval between a route being considered invalid and the route being purged from the routing table.

The basic timing parameters for IPv6 RIP are adjustable. Because IPv6 RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routers and access servers in the network.

Note The current and default timer values are displayed in the output of the **show ipv6 rip** EXEC command. The relationships of the various timers should be preserved, as described previously.

Examples

The following example sets updates to be broadcast every 5 seconds. If a route is not heard from in 15 seconds, the route is declared unusable. Further information is suppressed for an additional 10 seconds. Assuming no updates, the route is flushed from the routing table 20 seconds after the end of the hold-down period.

```
Router(config)# ipv6 router rip cisco
Router(config-rtr)# timers 5 15 10 30
```

Caution By setting a short update period, you run the risk of congesting slow-speed serial lines. Also, if you have many routes in your updates, you can cause the routers to spend an excessive amount of time processing updates.

Related Commands

Command	Description
show ipv6 rip	Displays information about current IPv6 RIP processes.

timers active-time

To adjust Enhanced Interior Gateway Routing Protocol (EIGRP) routing wait time, use the **timers active-time** command in router configuration mode or address-family topology configuration mode. To disable this function, use the **no** form of the command.

timers active-time [*time-limit* | **disabled**]

no timers active-time

Syntax Description

time-limit	(Optional) EIGRP active-time limit (in minutes). Valid range is 1 to 65535.
disabled	(Optional) Disables the timers and permits the routing wait time to remain active indefinitely.

Command Default

This command is disabled by default.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.4(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.
15.0(1)M	This command was modified. Address-family topology configuration mode was added. You must enter this command in address-family topology configuration mode for EIGRP named configurations.
12.2(33)SRE	This command was modified. Address-family topology configuration mode was added. You must enter this command in address-family topology configuration mode for EIGRP named configurations.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In EIGRP, there are timers that control the time that the router waits (after sending a query) before declaring the route to be in the stuck in active (SIA) state.

Examples

In the following example, the routing wait time is 200 minutes on the specified route:

```
Router(config)# router eigrp 5
Router(config-router)# timers active-time 200
```

In the following example, the routing wait time is 200 minutes on the specified address-family route:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# timers active-time 200
```

In the following example, the routing wait time is indefinite if a route becomes active:

```
Router(config)# router eigrp 5
Router(config-router)# timers active-time disabled
```

In the following example, the routing wait time is indefinite on the specified address-family route:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# timers active-time disabled
```

In the following example, the routing wait time is 100 minutes on the specified route:

```
Router(config)# ipv6 router eigrp 1
Router(config-router)# timers active-time 100
```

In the following example, the routing wait time is 100 minutes on the specified address-family route:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv6 autonomous-system 4453
Router(config-router-af)# topology base
Router(config-router-af-topology)# timers active-time disabled
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address-family configuration mode to configure an EIGRP routing instance.
ipv6 router eigrp	Configures the EIGRP IPv6 routing process.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address-family process.
show ip eigrp topology	Displays the EIGRP topology table.
show ipv6 eigrp topology	Displays the IPv6 EIGRP topology table.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address-family topology configuration mode.

timers lsa arrival

To set the minimum interval at which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First version 3 (OSPFv3) neighbors, use the **timers lsa arrival** command in OSPFv3 router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*

no timers lsa arrival

Syntax Description

milliseconds	Minimum delay in milliseconds that must pass between acceptance of the same LSA arriving from neighbors. The range is from 0 to 600,000 milliseconds. The default is 1000 milliseconds.

Defaults

1000 milliseconds

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.0(25)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped.

We suggest you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa all** command.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
router ospfv3 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
timers throttle lsa	Sets rate-limiting values for OSPFv3 LSA generation.
timers throttle lsa all	Sets rate-limiting values for LSAs being generated.

timers pacing flood (OSPFv3)

To configure link-state advertisement (LSA) flood packet pacing, use the **timers pacing flood** command in Open Shortest Path First version 3 (OSPFv3) router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*

no timers pacing flood

Syntax Description

milliseconds	Time (in milliseconds) at which LSAs in the flooding queue are paced in between updates. The configurable range is from 5 milliseconds to 100 milliseconds. The default value is 33 milliseconds.

Command Default

The default is 33 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.

Usage Guidelines

Configuring Open Shortest Path First version 3 (OSPF) flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 transmission queue. This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs.

The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer

summarization, stub area usage, queue tuning, and buffer tuning before changing the default flood timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default flood timer values.

Examples

The following example configures LSA flood packet-pacing updates to occur in 20-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing flood 20
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing lsa-group (OSPFv3)

To change the interval at which Open Shortest Path First version 3 (OSPFv3) link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers pacing lsa-group** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers pacing lsa-group *seconds*

no timers pacing lsa-group

Syntax Description

seconds	Number of seconds in the interval at which LSAs are grouped and refreshed, checksummed, or aged. The range is from 10 to 1800 seconds. The default value is 240 seconds.

Command Default

The default interval for this command is 240 seconds. OSPFv3 LSA group pacing is enabled by default.

Command Modes

OSPFv3 router configuration (config-router)

Command History

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

Usage Guidelines

This command allows you to control the rate at which LSA updates occur to reduce the high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes the risks associated with changing the default timer values.

Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group refreshment of LSAs; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh rate is every 30 minutes).

The duration of the LSA group pacing is inversely proportional to the number of LSAs the router is handling. For example, if you have about 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Examples

The following example configures OSPFv3 group packet-pacing updates between LSA groups to occur in 300-second intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing lsa-group 300
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission (OSPFv3)

To configure link-state advertisement (LSA) retransmission packet pacing in IPv4 Open Shortest Path First version 3 (OSPFv3), use the **timers pacing retransmission** command in OSPFv3 router configuration mode. To restore the default retransmission packet pacing value, use the **no** form of this command.

timers pacing retransmission *milliseconds*

no timers pacing retransmission

Syntax Description

milliseconds	The time (in milliseconds) at which LSAs in the retransmission queue are paced. The configurable range is from 5 milliseconds to 200 milliseconds. The default value is 66 milliseconds.

Command Default

The default is 66 milliseconds.

Command Modes

OSPFv3 router configuration (config-router)

Command History

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

Usage Guidelines

Configuring OSPFv3 retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPFv3 retransmission queue. This command allows you to control the rate at which LSA updates occur to reduce high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs. The default settings for OSPFv3 packet retransmission pacing timers are suitable for the majority of OSPFv3 deployments. Do not change the packet retransmission pacing timers unless all other options to meet OSPFv3 packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers. Furthermore, there are no guidelines for changing timer values; each OSPFv3 deployment is unique and should be considered on a case-by-case basis.

Note The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 100-millisecond intervals for OSPFv3 routing process 1:

```
Router(config)# router ospfv3 1
Router(config-router)# timers pacing retransmission 100
```

Related Commands

Command	Description
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.
timers pacing flood	Configures LSA flood packet pacing.
timers pacing lsa-group	Changes the interval at which OSPF LSAs are collected into a group and refreshed, checksummed, or aged.

timers register

To set how long the Session Initiation Protocol (SIP) user agent (UA) waits before sending register requests, use the **timers register** command in SIP user-agent configuration mode. To reset this value to the default, use the **no** form of this command.

timers register *milliseconds*

no timers register

Syntax Description

milliseconds	Waiting time, in milliseconds. Range is from 100 to 1000. Default is 500.

Defaults

500 milliseconds

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(22)T	Support for IPv6 was added.

Examples

The following example sends register requests every 500 milliseconds:

```
sip-ua
 retry invite 9
 retry register 9
 timers register 500
```

Related Commands

Command	Description
retry register	Sets the total number of SIP registers to send.

timers spf (IPv6)

To turn on Open Shortest Path First (OSPF) for IPv6 shortest path first (SPF) throttling, use the **timers spf** command in router configuration mode. To turn off SPF throttling, use the **no** form of this command.

timers spf *delay holdtime*

no timers spf

Syntax Description

delay	Delay (in milliseconds) in receiving a change in the SPF calculation. The range is from 0 through 4294967295. The default is 5 milliseconds.
holdtime	Hold time (in milliseconds) between consecutive SPF calculations. The range is from 0 through 4294967295. The default is 10 milliseconds.

Command Default

OSPF for IPv6 throttling is always enabled.

Command Modes

Router configuration

Command History

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

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *delay* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *holdtime* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Examples

The following example shows a router configured with the delay and hold-time interval values for the **timers spf** command set at 40 and 50 milliseconds, respectively.

```
Router(config)# ipv6 router ospf 1
Router(config-router)# timers spf 40 50
```

Related Commands

Command	Description
show ipv6 ospf	Displays general information about OSPF for IPv6 routing processes.

timers throttle lsa

To set rate-limiting values for Open Shortest Path First (OSPF) for IPv6 link-state advertisement (LSA) generation, use the **timers throttle lsa** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers throttle lsa *start-interval hold-interval max-interval*

no timers throttle lsa

Syntax Description

start-interval	Minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF for IPv6 topology change. The generation of the next LSA is not before the start interval. The range is from 0 to 600,000 milliseconds. The default is 0 milliseconds, which means no delay; the LSA is sent immediately.
hold-interval	Incremental time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Maximum wait time in milliseconds between generation of the same LSA. The range is from 1 to 600,000 milliseconds. The default value is 5000 milliseconds.

Defaults

start-interval: 0 milliseconds
hold-interval: 5000 milliseconds
max-interval: 5000 milliseconds

Command Modes

OSPF for IPv6 router configuration (config-rtr)
Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	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.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. We suggest you keep the *milliseconds* value of the **timers lsa arrival** command less than or equal to the *hold-interval* value of the **timers throttle lsa** command.

Examples

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

This example customizes IPv6 OSPF LSA throttling so that the start interval is 500 milliseconds, the hold interval is 1,000 milliseconds, and the maximum interval is 10,000 milliseconds.

```
ipv6 router ospf 1
 log-adjacency-changes
 timers throttle lsa 500 1000 10000
```

Related Commands

Command	Description
show ipv6 ospf	Displays information about OSPF for IPv6 routing processes.
timers lsa arrival	Sets the minimum interval at which the software accepts the same LSA from OSPF neighbors.

timers throttle spf

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the **timers throttle spf** command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the **no** form of this command.

timers throttle spf *spf-start spf-hold spf-max-wait*

no timers throttle spf *spf-start spf-hold spf-max-wait*

Syntax Description

spf-start	Initial delay to schedule an SFP calculation after a change, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 5000.
spf-hold	Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.
spf-max-wait	Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.

Command Default

SPF throttling is not set.

Command Modes

Address family configuration (config-router-af)
Router address family topology configuration (config-router-af-topology)
Router configuration (config-router)
OSPF for IPv6 router configuration (config-rtr)

Command History

Release	Modification
12.2(14)S	This command was introduced.This command replaces the **timers spf-interval** command.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was made available in router address family configuration mode.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	Support for IPv6 was added.
12.2(33)SB	Support for IPv6 was added and this command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Release	Modification
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the *spf-start* argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the *spf-max-wait* argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **timers throttle spf** command in router address family topology configuration mode in order to make this OSPF router configuration command become topology-aware.

Examples

The following example shows how to configure a router with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1000, and 90,000 milliseconds, respectively.

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 10.21.21.0 0.0.0.255 area 0
 network 10.22.22.0 0.0.0.255 area 00
```

The following example shows how to configure a router using IPv6 with the delay, hold, and maximum interval values for the **timers throttle spf** command set at 500, 1000, and 10,000 milliseconds, respectively.

```
ipv6 router ospf 1
 event-log size 10000 one-shot
 log-adjacency-changes
 timers throttle spf 500 1000 10000
```

traceroute

To discover the routes that packets will actually take when traveling to their destination address, use the **traceroute** command in user EXEC or privileged EXEC mode.

traceroute [**vrf** *vrf-name* | **topology** *topology-name*] [*protocol*] *destination*

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name of a Virtual Private Network (VPN) routing and forwarding (VRF) instance table in which to find the destination address. The only keyword that you can select for the *protocol* argument when you use the **vrf** *vrf-name* keyword-argument pair is the **ip** keyword.
topology *topology-name*	(Optional) Specifies the name of the topology instance. The *topology-name* argument is case-sensitive; "VOICE" and "voice" specify different topologies.
protocol	(Optional) Protocol keyword, either **appletalk**, **clns**, **ip**, **ipv6**, **ipx**, **oldvines**, or **vines**. When not specified, the *protocol* argument is based on an examination by the software of the format of the *destination* argument. The default protocol is IP.
destination	(Optional in privileged EXEC mode; required in user EXEC mode) The destination address or hostname for which you want to trace the route. The software determines the default parameters for the appropriate protocol and the tracing action begins.

Command Default

When not specified, the *protocol* argument is determined by the software examining the format of the *destination* argument. For example, if the software finds a *destination* argument in IP format, the protocol value defaults to IP.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The **vrf** *vrf-name* keyword and argument were added.
12.2(2)T	Support for IPv6 was added.
12.0(21)ST	Support for IPv6 was added.
12.0(22)S	Support for IPv6 was added.
12.2(11)T	The **traceroute** command test characters for IPv6 were updated. A new error message was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.3(5)	A line was added to the interactive **traceroute vrf** command, so that you can resolve the autonomous system number through the use of the global table or a VRF table, or you can choose not to resolve the autonomous system.
12.0(26)S1	Changes to the command were integrated into Cisco IOS Release 12.0(26)S1.
12.2(20)S	Changes to the command were integrated into Cisco IOS Release 12.2(20)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **topology** *topology-name* keyword and argument were added to support Multi-Topology Routing (MTR).
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2S	This command was modified. When the **vrf** keyword is used, the output displays the incoming VRF name/tag and the outgoing VRF name/tag.

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value.

The **traceroute** command starts by sending probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring routers to discard the probe datagram and send back an error message. The **traceroute** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A time-exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command terminates when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type **Ctrl-^ X**—by simultaneously pressing and releasing the **Ctrl**, **Shift**, and **6** keys, and then pressing the **X** key.

To use nondefault parameters and invoke an extended **traceroute** test, enter the command without a *protocol* or *destination* argument in privileged EXEC mode. You are stepped through a dialog to select the desired parameters. Extended **traceroute** tests are not supported in user EXEC mode. The user-level traceroute feature provides a basic trace facility for users who do not have system privileges. The *destination* argument is required in user EXEC mode.

If the system cannot map an address for a hostname, it returns a "%No valid source address for destination" message.

If the **vrf** *vrf-name* keyword and argument are used, the **topology** option is not displayed because only the default VRF is supported. The **topology** *topology-name* keyword and argument and the DiffServ Code Point (DSCP) option in the extended traceroute system dialog are displayed only if a topology is configured on the router.

In Cisco IOS XE Release 3.2S, output of the **traceroute** command with the **vrf** keyword was enhanced to make troubleshooting easier by displaying the incoming VRF name/tag and the outgoing VRF name/tag.

Examples

After you enter the **traceroute** command in privileged EXEC mode, the system prompts you for a protocol. The default protocol is IP.

If you enter a hostname or address on the same line as the **traceroute** command, the default action is taken as appropriate for the protocol type of that name or address.

The following example is sample dialog from the **traceroute** command using default values. The specific dialog varies somewhat from protocol to protocol.

```
Router# traceroute

Protocol [ip]:
Target IP address:
Source address:
DSCP Value [0]: ! Only displayed if a topology is configured on the router.
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose [none]:
```

The following example displays output available in Cisco IOS XE Release 3.2S and later. Output of the **traceroute** command with the **vrf** keyword includes the incoming VRF name/tag and the outgoing VRF name/tag.

```
Router# traceroute vrf red 10.0.10.12

Type escape sequence to abort.
Tracing the route to 10.0.10.12
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.13.15 (red/13,red/13) 0 msec
    10.1.16.16 (red/13,red/13) 0 msec
    10.1.13.15 (red/13,red/13) 1 msec
  2 10.1.8.13 (red/13,red/13) 0 msec
    10.1.7.13 (red/13,red/13) 0 msec
    10.1.8.13 (red/13,red/13) 0 msec
  3 10.1.2.11 (red/13,blue/10) 1 msec 0 msec 0 msec
  4  *  *  *
```

Related Commands

Command	Description
ping (MTR)	Pings a destination within a specific topology.

track interface

To configure an interface to be tracked and to enter tracking configuration mode, use the **track interface** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

no track *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

Syntax Description

object-number	Object number that represents the interface to be tracked. The range is from 1 to 1000.
type number	Interface type and number to be tracked. No space is required between the values.
line-protocol	Tracks the state of the interface line protocol.
ip routing	Tracks whether IP routing is enabled, whether an IP address is configured on the interface, and whether the interface state is up before reporting to the tracking client that the interface is up.

Command Default

No interface is tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **track interface ip routing** command was enhanced to allow the tracking of an IP address on an interface that was acquired through DHCP or PPP IPCP.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
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 integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

This command reports a state value to clients. A tracked IP-routing object is considered up when the following criteria exist:

- IP routing is enabled and active on the interface.
- The interface line-protocol state is up.
- The interface IP address in known. The IP address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.

Interface IP routing will go down when one of the following criteria exist:

- IP routing is disabled globally.
- The interface line-protocol state is down.
- The interface IP address is unknown. The IP address is not configured or received through DHCP or IPCP negotiation.

No space is required between the *type number* values.

Tracking the IP-routing state of an interface using the **track interface ip routing** command can be more useful in some situations than just tracking the line-protocol state using the **track interface line-protocol** command, especially on interfaces for which IP addresses are negotiated. For example, on a serial interface that uses the Point-to-Point Protocol (PPP), the line protocol could be up (link control protocol [LCP] negotiated successfully), but IP could be down (IPCP negotiation failed).

The **track interface ip routing** command supports the tracking of an interface with an IP address acquired through any of the following methods:

- Conventional IP address configuration
- PPP/IPCP
- DHCP
- Unnumbered interface

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0:

```
Router(config)# track 1 interface serial1/0 ip routing
Router(config-track)#
```

Related Commands

Command	Description
show track	Displays HSRP tracking information.

tracking

To override the default tracking policy on a port, use the **tracking** command in Neighbor Discovery (ND) inspection policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

Syntax Description

enable	Tracking is enabled.
reachable-lifetime	(Optional) The maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86,400 seconds, and the default is 300 seconds.
infinite	An entry is kept in a reachable or stale state for an infinite amount of time.
disable	Tracking is disabled.
stale-lifetime	(Optional) The time entry is kept in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

ND inspection policy configuration (config-nd-inspection)

Command History

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

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, one may not want to track entries but wants an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking, or indirectly through ND inspection. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **stale-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.
ipv6 neighbor tracking	Enables tracking of entries in the binding table.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

translation-profile (dial peer)

To assign a translation profile to a dial peer, use the **translation-profile** command in dial peer configuration mode. To delete the translation profile from the dial peer, use the **no** form of this command.

translation-profile {**incoming** | **outgoing**} *name*

no translation-profile {**incoming** | **outgoing**} *name*

Syntax Description

incoming	Specifies that this translation profile handles incoming calls.
outgoing	Specifies that this translation profile handles outgoing calls.
name	Name of the translation profile.

Defaults

No default behavior or values

Command Modes

Dial peer configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

Use the **translation-profile** command to assign a predefined translation profile to a dial peer.

Examples

The following example assigns the translation profile named "profile1" to handle translation of outgoing calls for a dial peer:

```
Router(config)# dial-peer voice 111 pots
Router(config-dial-peer)# translation-profile outgoing profile1
```

Related Commands

Command	Description
rule (voice translation-rule)	Sets the criteria for the translation rule.
show voice translation-profile	Displays the configuration of a translation profile.
translate (translation profiles)	Assigns a translation rule to a translation profile.
voice translation-profile	Initiates the translation-profile definition.
voice translation-rule	Initiates the translation-rule definition.

trusted-port (IPv6 ND Inspection Policy)

To configure a port to become a trusted port, use the **trusted-port** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

NDP inspection policy configuration (config-nd-inspection)

Command History

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

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Use the **trusted-port** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.

trusted-port (IPv6 RA Guard Policy)

To configure a port to become a trusted port, use the **trusted-port** command in router advertisement (RA) guard policy configuration. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

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

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, the **device-role** command takes precedence over the **trusted-port** command; if the device role is configured as host, messages will be dropped regardless of **trusted-port** command configuration.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-ra-guard)# trusted-port
```

Related Commands

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

tunnel 6rd br

To bypass security checks on an IPv6 rapid deployment (6RD) customer-edge (CE) router, use the **tunnel 6rd br command** in interface configuration mode. To remove the BR router's address from configuration, use the **no** form of this command.

tunnel 6rd br *ipv4-address*

no tunnel 6rd br *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the BR router.

Command Default

No BR router is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd br** command is optional for 6RD operation. The command allows the user to specify the BR address, which allows the 6RD router to skip the security checks for packets from that source.

By default at a 6RD router, all incoming packets require that their outer IPv4 source address to be embedded in the 6RD-encoded IPv6 source address. Packets that do not satisfy this criteria are dropped. Configuring the **tunnel 6rd br** command exempts packets with the specified source from this check.

The **tunnel 6rd br** command should be enabled on the customer edge (CE) router, because packets arriving at the CE from the BR typically are traffic from a native IPv6 host, which does not need to have a 6RD-encoded source address.

Examples

The following example sets the BR address to 10.1.4.1:

```
Router(config-if)# tunnel 6rd br 10.1.4.1
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

Command	Description
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd ipv4

To specify the prefix length and suffix length of the IPv4 transport address common to all the 6RD routers in a domain, use the **tunnel 6rd ipv4** command in interface configuration mode. To remove these parameters, use the **no** form of this command.

tunnel 6rd ipv4 {**prefix-len** *length*} {**suffix-len** *length*}

no tunnel 6rd ipv4 {**prefix-len** *length*} {**suffix-len** *length*}

Syntax Description

prefix-len *length*	Specifies the prefix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.
suffix-len *length*	Specifies the suffix length, in bits, common to all 6RD routers in a domain. • The range is from 0 to 31, and the default is 0. • The sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31.

Command Default

The prefix length and suffix length are 0.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd ipv4** command is optional for 6RD operation. This command specifies the number of most significant bits and least significant bits of the IPv4 transport address (that is, the tunnel source) that are common to all the 6RD routers in a domain. The valid range is from 0 to 31, and the sum of the IPv4 prefix length and the IPv4 suffix length cannot exceed 31. If the **tunnel 6rd ipv4** command is not configured, and the **tunnel 6rd prefix** command is configured, the system uses the default value of 0.

Examples

The following example shows 6RD configuration, including the number of most and least significant bits of the IPv4 transport address common to all the 6RD routers in a domain:

```
Router(config)# interface Tunnel1
Router(config-if)# ipv6 address 2001:B000:100::1/32
Router(config-if)# tunnel source GigabitEthernet2/0/0
Router(config-if)# tunnel mode ipv6ip 6rd
Router(config-if)# tunnel 6rd prefix 2001:B000::/32
```

```
Router(config-if)# tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel 6rd prefix	Specifies the common IPv6 prefix on 6RD tunnels
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel 6rd prefix

To specify the common IPv6 prefix on IPv6 rapid deployment (6RD) tunnels, use the **tunnel 6rd prefix** command in interface configuration mode. To remove the IPv6 prefix, use the **no** form of this command.

tunnel 6rd prefix *ipv6-prefix*/*prefix-length*

no tunnel 6rd prefix *ipv6-prefix*/*prefix-length*

Syntax Description

ipv6-prefix	The IPv6 network assigned to the general prefix. 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*	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.

Command Default

This command can be enabled only when 6RD is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

The **tunnel 6rd prefix** command is mandatory for 6RD operation. It specifies the common IPv6 prefix, and the *prefix-length* argument determines us the position of the IPv4 address in the 6RD delegated prefix (or payload) destination. Configuring a *prefix-length* of 0 is equivalent to removing this command.

The tunnel line state of a 6RD tunnel remains inactive until the **tunnel 6rd prefix** command is configured, and this command is automatically disabled when the **tunnel mode ipv6ip** command is configured to use a keyword other than **6rd**.

Examples

The following example shows 6RD configuration, including the **tunnel 6rd prefix** command:

```
ipv6 general-prefix 6rd1 6rd Tunnel1
!
interface Tunnel1
 ipv6 address 6rd1 ::1/124
tunnel source GigabitEthernet2/0/0
tunnel mode ipv6ip 6rd
tunnel 6rd prefix 2001:B000::/32
tunnel 6rd ipv4 prefix-len 16 suffix-len 8
```

Related Commands

Command	Description
ip address	Specifies the IPv4 address of an IPv4 interface.
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

tunnel destination {*host-name* | *ip-address* | *ipv6-address*}

no tunnel destination

Syntax Description

host-name	Name of the host destination.
ip-address	IP address of the host destination expressed in dotted decimal notation.
ipv6-address	IPv6 address of the host destination expressed in IPv6 address format.

Command Default

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The address field was modified to accept an *ipv6-address* argument to allow IPv6 nodes to be configured as a tunnel destination.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and configure the packet source off of the loopback interface. Refer to the *Cisco IOS AppleTalk*, *DECnet*, *ISO CLNS*, *and Novell IPX Configuration Guide* for more information on AppleTalk Cayman tunneling.

Examples

Tunnel Destination Address for Cayman Tunnel Example

The following example shows how to configure the tunnel destination address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
```

```
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

Tunnel Destination Address for GRE Tunneling Example

The following generic routing encapsulation (GRE) example shows how to configure the tunnel destination address for GRE tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

Tunnel Destination Address for IPv6 Tunnel Example

The following GRE example shows how to configure the tunnel destination address for GRE tunneling of IPv6 packets:

```
Router(config)# interface Tunnel0
Router(config-if)#  no ip address
Router(config-if)#  ipv6 router isis
Router(config-if)#  tunnel source Ethernet0/0
Router(config-if)#  tunnel destination 2001:0DB8:1111:2222::1/64
Router(config-if)#  tunnel mode gre ipv6
Router(config-if)# exit
!
Router(config)# interface Ethernet0/0
Router(config-if)#  ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
!
Router(config)# ipv6 unicast-routing

Router(config)# router isis
Router(config)#  net 49.0000.0000.000a.00
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel source	Sets the source address of a tunnel interface.

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the **no** form of this command.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}

no tunnel mode

Syntax Description

aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible Connectionless Network Protocol (CLNS) tunnel.
gre	Generic routing encapsulation (GRE) protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
gre ipv6	GRE tunneling using IPv6 as the delivery protocol.
ipip	IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Tunnel mode is IPSec, and the transport is IPv4.
iptalk	Apple IPTalk encapsulation.
ipv6	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
ipsec ipv6	Tunnel mode is IPSec, and the transport is IPv6.
mpls	Multiprotocol Label Switching (MPLS) encapsulation.
nos	KA9Q/NOS compatible IP over IP.
rbscp	Rate Based Satellite Control Protocol (RBSCP).

Command Default

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **aurp**, **dvmrp**, and **ipip** keywords were added.
11.2	The optional **decapsulate-any** keyword was added.
12.2(13)T	The **gre multipoint** keyword was added.

Release	Modification
12.3(7)T	The following keywords were added: • **gre ipv6** to support GRE tunneling using IPv6 as the delivery protocol. • **ipv6** to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • **rbscp** to support RBSCP.
12.3(14)T	The **ipsec ipv4** keyword was added.
12.2(18)SXE	The **gre multipoint** keyword added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	The **ipsec ipv6** keyword 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

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mrouted (multicast) router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPSec profile. Combining mGRE tunnels and IPSec encryption allows a single mGRE interface to support multiple IPSec tunnels, thereby simplifying the size and complexity of the configuration.

Note GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPSec, over satellite links without breaking the end-to-end model.

IPSec in IPv6 Transport

IPv6 IPSec encapsulation provides site-to-site IPSec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 routers to work as a security gateway, establishes IPSec tunnels between another security gateway router, and provides crypto IPSec protection for traffic from an internal network when being transmitting across the public IPv6 Internet. IPv6 IPSec is very similar to the security gateway model using IPv4 IPsec protection.

Examples

Cayman Tunneling

The following example shows how to enable Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

GRE Tunneling

The following example shows how to enable GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre
```

IPSec in IPv4 Transport

The following example shows how to configure a tunnel using IPSec encapsulation with IPv4 as the transport mechanism:

```
Router(config)# crypto ipsec profile PROF
Router(config)#  set transform tset
Router(config)# interface Tunnel0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel source Loopback0
Router(config-if)# tunnel destination 172.16.1.1
Router(config-if)# tunnel protection ipsec profile PROF
```

IPSec in IPv6 Transport

The following example shows how to configure an IPv6 IPSec tunnel interface:

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Router(config-if)# tunnel destination 10.0.0.1
Router(config-if)# tunnel source Ethernet 0/0
Router(config-if)# tunnel mode ipsec ipv6
Router(config-if)# tunnel protection ipsec profile profile1
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
 ip mtu 1416
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets IPSec peer address to Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

RBSCP Tunneling

The following example shows how to enable RBSCP tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel mode ipv6ip

To configure a static IPv6 tunnel interface, use the **tunnel mode ipv6ip** command in interface configuration mode. To remove an IPv6 tunnel interface, use the **no** form of this command.

tunnel mode ipv6ip [**6rd** | **6to4** | **auto-tunnel** | **isatap**]

no tunnel mode ipv6ip

Syntax Description

6rd	(Optional) Specifies that the tunnel is to be used for IPv6 rapid deployment (6RD).
6to4	(Optional) Specifies IPv6 automatic tunneling mode using a 6to4 address.
auto-tunnel	(Optional) Specifies IPv6 automatic tunneling mode using an IPv4-compatible IPv6 address.
isatap	(Optional) Specifies IPv6 automatic tunneling mode as Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) to connect IPv6 nodes (hosts and routers) within IPv4 networks.

Command Default

IPv6 tunnel interfaces are not configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	The ISATAP keyword was added to support the addition of ISATAP tunnel implementation.
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.
Cisco IOS XE Release 3.1S	The **6rd** keyword was added. The **auto-tunnel** keyword is not supported on Cisco ASR 1000 series routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.
15.0(1)SY	This command is not supported as of Cisco IOS Release 15.0(1)SY.

Usage Guidelines

IPv6 tunneling consists of encapsulating IPv6 packets within IPv4 packets for transmission across an IPv4 routing infrastructure.

Manually Configured Tunnels

Using the **tunnel mode ipv6ip** command without keywords specifies an IPv6 configured tunnel where a manually configured IPv6 address is configured on a tunnel interface and manually configured IPv4 addresses are configured as the tunnel source and the tunnel destination. The host or router at each end of an IPv6 configured tunnel must support both the IPv4 and IPv6 protocol stacks.

Automatic Determination of Tunnel Source and Destination

Using the **tunnel mode ipv6ip** command with the **auto-tunnel** keyword specifies an IPv6 automatic tunnel where the tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses. An IPv4-compatible IPv6 address is a 128-bit IPv6 address that contains the IPv6 prefix 0:0:0:0:0:0 in the high-order 96 bits of the address and an IPv4 address in the low-order 32 bits of the address. The host or router at each end of an automatic tunnel must support both the IPv4 and IPv6 protocol stacks.

6to4 Tunnels

Using the **tunnel mode ipv6ip** command with the **6to4** keyword specifies automatic 6to4 tunneling where the tunnel endpoint is determined by the globally unique IPv4 address embedded in a 6to4 address. A 6to4 address is a combination of the prefix 2002::/16 and a globally unique 32-bit IPv4 address. (IPv4-compatible addresses are not used in 6to4 tunneling.) The unique IPv4 address is used as the network-layer address in the 6to4 address prefix. The border router at each end of a 6to4 tunnel must support both the IPv4 and IPv6 protocol stacks. The 6to4 tunnel must be configured with the **tunnel source** command to use an interface with an IPv4 address as the source of the tunnel. Additionally, the 6to4 address prefix must be routed over the tunnel using the **ipv6 route** command.

6RD Tunnels

Use the **tunnel mode ipv6ip** command with the **6rd** keyword specifies that the tunnel is to be used for IPv6 RD. The 6RD feature is similar to the 6to4 tunnel feature but it does not require addresses to have a 2002::/16 prefix nor does it require that all the 32 bits of the IPv4 destination be in the IPv6 payload header.

ISATAP Tunnels

ISATAP tunnels enable transport of IPv6 packets within network boundaries. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure.

Unlike IPv4-compatible addresses, ISATAP IPv6 addresses can use any initial unicast /64 prefix. The final 64 bits are an interface identifier. Of these, the leading 32 bits are the fixed pattern 0000:5EFE; the last 32 bits carry the tunnel endpoint IPv4 address.

Examples

Manually Configured IPv6 Tunnel Example

The following example configures a manual IPv6 tunnel. In the example, tunnel interface 0 is manually configured with a global IPv6 address. The tunnel source and destination are also manually configured.

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 192.168.30.1
Router(config-if)# tunnel mode ipv6ip
```

IPv4 Compatible IPv6 Address Tunnel Example

The following example configures an automatic IPv6 tunnel that uses Ethernet interface 0 as the tunnel source. The tunnel destination is automatically determined by the IPv4 address in the low-order 32 bits of an IPv4-compatible IPv6 address.

```
Router(config)# interface tunnel 0
Router(config-if)# no ip address
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip auto-tunnel
```

6to4 Tunnel Example

The following example configures a 6to4 tunnel. 6to4 tunnels allows for autoconfiguration where a site-specific 48-bit prefix is dynamically constructed by prepending the prefix 2002 to an IPv4 address assigned to the site. In the example, Ethernet interface 0 is configured with an IPv4 address, and with a 64-bit prefix (/64) which is part of the previously constructed 48-bit prefix (/48). Tunnel interface 0 is configured without an IPv4 or IPv6 address because the IPv4 or IPv6 addresses on Ethernet interface 0 is used to construct a tunnel source address. A tunnel destination address is not specified because the destination address is automatically constructed. An IPv6 static route for network 2002::/16 to tunnel interface 0 is configured (traffic destined for the prefix is routed over tunnel interface 0).

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 192.168.99.1 255.255.255.0
Router(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Router(config-if)# exit
Router(config)# interface tunnel 0
Router(config-if)# no ip address
Router(config-if)# ipv6 unnumbered ethernet 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip 6to4
Router(config-if)# exit
Router(config)# ipv6 route 2002::/16 tunnel 0
```

Tunnel Interface Configured with the ipv6 unnumbered Command Example

When a tunnel interface is configured using the **ipv6 unnumbered** command with the **tunnel source** and **tunnel mode ipv6ip** commands, the tunnel uses the first IPv6 address configured on the source interface as its IPv6 address. For 6to4 tunnels, the first IPv6 address configured on the source interface must be a 6to4 address. In the following example, the first IPv6 address configured for Ethernet interface 0 (6to4 address 2002:c0a8:6301:1::/64) is used as the IPv6 address of tunnel 0:

```
Router(config)# interface tunnel 0
Router(config-if)# ipv6 unnumbered ethernet 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip 6to4
Router(config-if)# exit
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2002:c0a8:6301:1::/64 eui-64
Router(config-if)# ipv6 address 3ffe:1234:5678::1/64
```

6RD Tunnel Example

The following sample output shows the running configuration of a 6RD tunnel:

```
Router(config)# interface Tunnel1
Router(config-if)# ipv6 address 2001:B000:100::1/32
Router(config-if)# tunnel source GigabitEthernet2/0/0
Router(config-if)# tunnel mode ipv6ip 6rd
Router(config-if)# tunnel 6rd prefix 2001:B000::/32
Router(config-if)# tunnel 6rd common prefix-len 16 suffix-len 8

Router# show tunnel 6rd tunnel
```

```
Interface Tunnel1:
  Tunnel Source: 10.1.1.1
  6RD: Operational, V6 Prefix: 2001:B000::/32
       V4 Common Prefix Length: 16, Value: 10.1.0.0
       V4 Common Suffix Length: 8, Value: 0.0.0.1
```

ISATAP Tunnel Example

The following command shows an ISATAP tunnel configured on interface Ethernet 0. Router advertisements are enabled to allow client autoconfiguration.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config)# interface Tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode ipv6ip isatap
Router(config-if)# ipv6 address 2001:0DB8::/64 eiu-64
Router(config-if)# no ipv6 nd suppress-ra
```

Related Commands

Command	Description
ip address	Specifies the IP address of an IPv4 interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.
tunnel destination	Sets the destination address for a tunnel interface.
tunnel source	Sets the source address for a tunnel interface.

tunnel source

To set the source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source {*ip-address* | *ipv6-address* | *interface-type interface-number*}

no tunnel source

Syntax Description

ip-address	IP address to use as the source address for packets in the tunnel. • In the case of traffic engineering (TE) tunnels it is the control packets that are affected.
ipv6-address	IPv6 address to use as the source address for packets in the tunnel.
interface-type	Interface type.
interface-number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command.

Command Default

No tunnel interface source address is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The address field has been updated to accept IPv6 addresses as the source address to allow an IPv6 node to be used as a tunnel source.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The source address is either an explicitly defined IP address or the IP address assigned to the specified interface.

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface. This restriction is applicable only for generic routing encapsulation (GRE) tunnels. You can have more than one TE tunnel with the same source and destination address.

When using tunnels to Cayman boxes, you must set the **tunnel source** command to an explicit IP address on the same subnet as the Cayman box, not the tunnel itself.

GRE tunnel encapsulation and deencapsulation for multicast packets are handled by the hardware in PFC3 and 12.2(18)SXF and later releases. Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. You should use secondary addresses on loopback interfaces or create multiple loopback interfaces to ensure the hardware-assisted tunnels do not share a source.

Examples

Cayman Tunnel Example

The following example shows how to set a tunnel source address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.32.164.19
Router(config-if)# tunnel mode cisco1
```

GRE Tunneling Example

The following example shows how to set a tunnel source address for GRE tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.32.164.19
Router(config-if)# tunnel mode gre ip
```

MPLS TE Tunnel Example

The following example shows how to set a tunnel source for a Multiprotocol Label Switching (MPLS) TE tunnel:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel source loopback1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# end
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.

validate source-mac

To check the source media access control (MAC) address against the link-layer address, use the **validate source-mac** command in Neighbor Discovery (ND) inspection policy configuration mode.

validate source-mac

no validate source-mac

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

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

When the router receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. Use the **validate source-mac** command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Examples

The following example enables the router to drop an ND message whose link-layer address does not match the MAC address:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# validate source-mac
```

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.

variance (EIGRP)

To control load balancing in an internetwork based on the Enhanced Interior Gateway Routing Protocol (EIGRP), use the **variance** command in router configuration mode or address-family topology configuration mode. To reset the variance to the default value, use the **no** form of this command.

variance *multiplier*

no variance

Syntax Description

multiplier	Metric value used for load balancing. It can be a value from 1 to 128. The default is 1, which means equal-cost load balancing.

Command Default

EIGRP uses equal-cost load balancing.

Command Modes

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

Command History

Release	Modification
10.0	This command was introduced.
12.4(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.
15.0(1)	This command was modified. Address-family topology configuration mode was added.
12.2(33)SRE	This command was modified. Address-family topology configuration mode was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Setting a variance value enables EIGRP to install multiple loop-free routes with unequal cost in a local routing table. A route learned through EIGRP must meet two criteria to be installed in the local routing table:

- The route must be loop- free. This condition is satisfied when the reported distance is less than the total distance or when the route is a feasible successor.
- The metric of the route must be lower than the metric of the best route (the successor) multiplied by the variance configured on the router.

Thus, if the variance is set to 1, only routes with the same metric as the successor are installed in the local routing table. If the variance is set to 2, any EIGRP-learned route with a metric less than 2 times the successor metric will be installed in the local routing table.

Note EIGRP does not load-share between multiple routes; it only installs the routes in the local routing table. Then, the local routing table enables switching hardware or software to load-share between the multiple paths.

Examples

The following example sets a variance value of 4:

```
Router(config)# router eigrp 109
Router(config-router)# variance 4
```

The following example sets a variance value of 4 in address-family topology configuration mode:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# variance 4
```

virtual-profile virtual-template

To enable virtual profiles by virtual interface template, use the **virtual-profile virtual-template** command in global configuration mode. To disable this function, use the **no** form of this command.

virtual-profile virtual-template *number*

no virtual-profile virtual-template *number*

Syntax Description

number	Number of the virtual template to apply, ranging from 1 to 30.

Defaults

Disabled. No virtual template is defined, and no default virtual template number is used.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

When virtual profiles are configured by virtual templates only, any interface-specific configuration information that is downloaded from the AAA server is ignored in configuring the virtual access interface for a user.

The **interface virtual-template** command defines a virtual template to be used for virtual profiles. Because several virtual templates might be defined for different purposes on the router (such as MLP, PPP over ATM, and virtual profiles), it is important to be clear about the virtual template number to use in each case.

Examples

The following example configures virtual profiles by virtual templates only. The number 2 was chosen because virtual template 1 was previously defined for use by Multilink PPP.

```
virtual-profile virtual-template 2
```

Related Commands

Command	Description
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces.

voice-class sip anat

To enable Alternative Network Address Types (ANAT) on a Session Initiation Protocol (SIP) trunk, use the **voice-class sip anat** command in SIP configuration or dial peer configuration mode. To disable ANAT on SIP trunks, use the **no** form of this command.

voice-class sip anat [**system**]

no voice-class sip anat [**system**]

Syntax Description

system	(Optional) Configures ANAT globally.

Command Default

ANAT is enabled on SIP trunks.

Command Modes

SIP configuration (conf-serv-sip)
Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Both the Cisco IOS SIP gateway and Cisco Unified Border Element are required to support the Session Description Protocol (SDP) ANAT semantics. The **bind** command allows the use of ANAT semantics in outbound SDP. SDP ANAT semantics are intended to address scenarios that involve different network address families (for example, different IPv4 versions). Media lines grouped using ANAT semantics provide alternative network addresses of different families for a single logical media stream. The entity creating a session description with an ANAT group must be ready to receive or send media over any of the grouped "m" lines.

By default, ANAT is enabled on SIP trunks. However, if the SIP gateway is configured in IPv4-only mode or IPv6-only mode, the gateway will not use ANAT semantics in its SDP offer.

The **system** keyword configures ANAT on all network dial peers, including the local dial peer. Using the **voice-class sip anat** command without the **system** keyword enables ANAT only for the local dial peer.

Examples

The following example globally enables ANAT on a SIP trunk:

```
Router(config-serv-sip)# voice-class sip anat system
```

The following example enables ANAT on a specified dial peer:

```
Router(config-dial-peer)# voice-class sip anat
```

Related Commands

Command	Description
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.

voice-class sip outbound-proxy

To configure an outbound proxy, use the **voice-class sip outbound-proxy** command in dial peer configuration mode. To reset the outbound proxy value to its default, use the **no** form of this command.

voice-class sip outbound-proxy {**dhcp** | **ipv4:***ipv4-address* | **ipv6:[***ipv6-address***]** | **dns:***host***:***domain*} [**:***port-number*]

no voice-class sip outbound-proxy

Syntax Description

dhcp	Specifies that the outbound-proxy IP address is retrieved from a DHCP server.
ipv4:*ipv4-address*	Configures proxy on the server, sending all initiating requests to the specified IPv4 address destination. The colon is required.
ipv6:[*ipv6-address***]**	Configures proxy on the server, sending all initiating requests to the specified IPv6 address destination. Brackets must be entered around the IPv6 address. The colon is required.
dns:*host***:***domain*	Configures proxy on the server, sending all initiating requests to the specified domain destination. The colons are required.
:*port-number*	(Optional) Port number for the Session Initiation Protocol (SIP) server. The colon is required.

Command Default

An outbound proxy is not configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(15)T	This command was introduced.
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 in Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **voice-class sip outbound-proxy** command, in dial peer configuration mode, takes precedence over the command in SIP global configuration mode.

Brackets must be entered around the IPv6 address.

Examples

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate an IPv4 address (10.1.1.1) as an outbound proxy:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy ipv4:10.1.1.1
```

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate a domain (sipproxy:cisco.com) as an outbound proxy:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dns:sipproxy:cisco.com
```

The following example shows how to configure the **voice-class sip outbound-proxy** command on a dial peer to generate an outbound proxy using DHCP:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
voice service	Enters voice-service configuration mode and specifies a voice encapsulation type.

voice-class source interface

To allow a loopback interface to be associated with a VoIP or VoIPv6 dial-peer profile, use the **voice-class source interface** command in dial peer configuration mode. To disable this association, use the **no** form of this command.

voice-class source interface loopback *interface-id* [*ipv4-address* | *ipv6-address*]

no voice-class source interface loopback *interface-id* [*ipv4-address* | *ipv6-address*]

Syntax Description

loopback	Specifies the loopback interface address.
interface-id	Specifies the interface on which the address is to be configured.
ipv4-address	(Optional) IPv4 address used in the loopback interface address.
ipv6-address	(Optional) IPv6 address used in the loopback interface address.

Command Default

No loopback interface is associated with a VoIPv6 dial-peer profile.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

When the **voice-class source interface** command is configured, the source address of Routing Table Protocol (RTP) generated by the gateway is taken from the address configured under the loopback interface. This command is used for policy-based routing (PBR) of voice packets originated by the gateway. The policy route map is configured under the loopback interface, and then the loopback interface is specified under the VoIP or VoIPv6 dial peer.

Examples

The following example associates a loopback interface with a VoIPv6 dial-peer profile:

```
Router(config)# dial-peer voice 1 voip
Router (config-dial-peer)# voice-class source interface loopback0
```

Related Commands

Command	Description
dial-peer voice	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

voice service

To enter voice-service configuration mode and to specify a voice-encapsulation type, use the voice service command in global configuration mode..

voice service {**pots** | **voatm** | **vofr** | **voip**}

Syntax Description

pots	Telephony voice service.
voatm	Voice over ATM (VoATM) encapsulation.
vofr	Voice over Frame Relay (VoFR) encapsulation.
voip	Voice over IP (VoIP) encapsulation.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T for VoIP on the Cisco 2600 series and the Cisco 3600 series.
12.1(3)XI	This command was implemented on the Cisco AS5300.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	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(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

Voice-service configuration mode is used for packet telephony service commands that affect the gateway globally.

Examples

The following example enters voice-service configuration mode for VoATM service commands:

```
voice service voatm
```

vpn

To specify that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **vpn** command in VPDN group or VPDN template configuration mode. To disassociate all IPv4 addresses in a VPDN group from a VRF, use the **no** form of this command.

vpn {**vrf** *vrf-name* | **id** *vpn-id*}

no vpn

Syntax Description

vrf *vrf-name*	Name of the VRF instance to be associated with the IPv4 addresses of the VPDN group.
id *vpn-id*	VPN ID of the VRF to be associated with the IPv4 addresses of the VPDN group.

Command Default

VPDN groups are not associated with a VRF.

Command Modes

VPDN group configuration
VPDN template configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)XI7	This command was integrated into Cisco IOS Release 12.3(7)XI7 and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB for the PRE2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was implemented on the Cisco 10000 series router for the PRE3.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **vpn** command to configure the Cisco IOS software to look up a VPDN source or destination IPv4 address in a specific VPN routing table instead of the global routing table.

Before you can issue the **vpn** command, a VRF instance must be created using the **ip vrf** command.

The **vpn** command can be used with both dial-in and dial-out VPDN scenarios.

Examples

The following example associates the IP addresses configured in the VPDN group named group1 with the VRF named vrf-second:

```
vpdn-group group1
```

```
 request-dialin
 protocol l2tp
!
 vpn vrf vrf-second
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

The following example associates the IP addresses configured in the VPDN group named group2 with the VPN ID 11:2222:

```
vpdn-group group2
 request-dialin
 protocol l2tp
!
 vpn id 11:2222
 source-ip 172.16.1.9
 initiate-to ip 172.16.1.1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip route	Displays all static IP routes, or those installed using the AAA route download function.
show vpdn session	Displays session information about active Layer 2 sessions for a VPDN.
show vpdn tunnel	Displays information about active Layer 2 tunnels for a VPDN.
vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
vpdn-template	Creates a VPDN template and enters VPDN template configuration mode.

vrf (DHCPv6 pool)

To associate a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address pool with a virtual private network (VPN) routing and forwarding (VRF) instance, use the **vrf** command in DHCPv6 pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

name	Name of the VRF with which the address pool is associated.

Command Default

No VRF is associated with the DHCPv6 address pool.

Command Modes

DHCPv6 pool configuration (config-dhcp)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Examples

The following example shows how to configure an IPv6 pool named pool1, and associate pool1 with a VRF instance named vrf1:

```
Router(config)# ipv6 dhcp pool pool1
# vrf vrf1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.

vrf definition

To configure a virtual routing and forwarding (VRF) routing table instance and enter VRF configuration mode, use the **vrf definition** command in global configuration mode. To remove a VRF routing table, use the **no** form of this command.

vrf definition *vrf-name*

no vrf definition *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined.
No import or export lists are associated with a VRF.
No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2S	This command was modified. Its use was expanded to support virtual networks.

Usage Guidelines

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. Once the router is in VRF configuration mode, use the **rd** command to give the VRF a route distinguisher (RD). The **rd** command creates the routing and forwarding tables and associates the RD with the VRF instance named in the *vrf-name* argument.

Users can configure shared route targets (import and export) between IPv4 and IPv6. This feature is useful in a migration scenario, where IPv4 policies already are configured and IPv6 policies should be the same as the IPv4 policies. You can configure separate route-target policies for IPv4 and IPv6 VPNs in address family configuration mode. Enter address family configuration mode from VRF configuration mode.

In VRF configuration mode, you can also associate a Simple Network Management Protocol (SNMP) context with the named VRF and configure or update a VPN ID.

The **vrf definition default** command can be used to configure a VRF name that is a NULL value until a default VRF name can be configured. This is typically before any VRF-related AAA commands are configured.

Virtual Network Use of vrf definition Command

Use the **vrf definition** command to give a VRF a name and to enter VRF configuration mode. By default, each virtual network trunk interface on the router is able to carry traffic for every VRF defined by the **vrf definition** command. If you want to enable only a subset of VRFs on a trunk interface, use the **vrf list** command.

Note We recommend you do not define a virtual network with the name "global," because the system predefines **vnet globa**l and it is best to avoid conflict with the predefined version.

Examples

The following example assigns the name vrf1 to a VRF, enters VRF configuration mode, and configures a route distinguisher, 100:20:

```
Router(config)# vrf definition vrf1
Router(config-vrf)# rd 100:20
```

The following virtual network example defines VRF red, enters VRF configuration mode, and assigns virtual network tag 100 to VRF red:

```
Router(config)# vrf definition red
Router(config-vrf)# vnet tag 100
```

Related Commands

Command	Description
address-family (VRF)	Enters VRF address family configuration mode to select an address family type for a VRF table.
context	Associates an SNMP context with a particular VRF.
rd	Specifies a route distinguisher.
route-target	Creates a route-target extended community for a VPN VRF.
vnet	Configures overrides of an interface's attributes on a per-VRF basis
vnet tag	Assigns a tag to a virtual network.
vpn id	Sets or updates a VPN ID on a VRF.
vrf forwarding	Associates a VRF instance with an interface or subinterface.
vrf list	Defines a list of VRFs.

vrf forwarding

To associate a Virtual Routing and Forwarding (VRF) instance or a virtual network with an interface or subinterface, use the **vrf forwarding** command in interface configuration mode. To disassociate a VRF or virtual network from an interface, use the **no** form of this command.

vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

no vrf forwarding

Syntax Description

vrf-name	The interface name to be associated with the specified VRF.
downstream	(Optional) Enables half-duplex VRF (HDVRF) functionality on the interface and associates the interface with the downstream VRF.
vrf-name2	(Optional) The interface name to be associated with the specified downstream VRF.

Command Default

The default for an interface is the global routing table.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
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. The **downstream** *vrf-name2* keyword and argument were added to support Multiprotocol Label Switching VPN half-duplex VRFs.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.2S	This command was modified. Its use was expanded to support virtual networks.

Usage Guidelines

Use the **vrf forwarding** command to associate an interface with a VRF. When the interface is bound to a VRF, previously configured IPv4 and IPv6 addresses are removed, and they must be reconfigured.

The **downstream** keyword associates the interfaces with a downstream VRF, which enables half-duplex VRF functionality on the interface. Some functions operate in the upstream VRFs, and others operate in the downstream VRFs. The following functions operate in the downstream VRFs:

- PPP peer routes are installed in the downstream VRFs.
- Authentication, authorization, and accounting (AAA) per-user routes are installed in the downstream VRFs.

- A Reverse Path Forwarding (RPF) check is performed in the downstream VRFs.

In the virtual network environment, the **vrf forwarding** command is supported on an edge interface; it is not supported on a trunk interface.

A VRF and a virtual network are mutually exclusive on an interface. In other words, an interface can be a VRF interface or a virtual network edge interface, but not both.

Examples

The following example shows how to associate a VRF named site1 to serial interface 0/0 and configure an IPv6 and an IPv4 address:

```
interface Serial0/0
 vrf forwarding site1
 ipv6 address 2001:100:1:1000::72b/64
 ip address 10.11.11.1 255.255.255.0
```

The following example associates the VRF named U with the virtual-template 1 interface and specifies the downstream VRF named D:

```
Router(config)# interface virtual-template 1
Router(config-if)# vrf forwarding U downstream D
Router(config-if)# ip unnumbered Loopback1
```

The following example shows how to configure an edge interface:

```
interface gigabitethernet 0/0/0
 vrf forwarding red
 ip address 10.12.12.1 255.255.255.0
```

Related Commands

Command	Description
vnet	Enters virtual network interface mode.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

zone security {*zone-name* | **default**}

no zone security {*zone-name* | **default**}

Syntax Description

zone-name	Name of the security zone. You can enter up to 256 alphanumeric characters.
default	Specifies the name of a default security zone. Interfaces that are not configured on any of the security zones belong to the default zone.

Command Default

There is a system-defined “self” zone.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was modified. The **default** keyword was added.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

We recommend that you create at least two security zones so that you can create a zone pair. If you create only one zone, you can use the default system-defined self zone. The self zone cannot be used for traffic going through a router. You can specify the **default** keyword to include all the interfaces that are not configured with any other zones.

To configure an interface to be a member of a security zone, use the **zone-member security** command.

Examples

The following example shows how to create and describe zones x1 and z1:

```
zone security x1
 description testzonex

zone security z1
 description testzonez
```

The following example shows how to create a default zone:

```
zone security default
 description system level default zone
```

Related Commands

Command	Description
description (identify zone)	Contains a description of a zone.
zone-member security	Attaches an interface to a zone.
zone-pair security	Creates a zonepair.

zone pair security

To create a zone pair, use the **zone-pair security** command in global configuration mode. To delete a zone pair, use the **no** form of this command.

zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}

no zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}

Syntax Description

zone-pair-name	Name of the zone being attached to an interface.
source *source-zone-name*	Specifies the name of the router from which traffic is originating.
default	Specifies the name of the default security zone. Interfaces without configured zones belong to the default zone.
destination *destination-zone-name*	Specifies the name of the router to which traffic is bound.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from a router.

Command Default

A zone pair is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was modified. The **default** keyword was added.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

This command creates a zone-pair, which permits a unidirectional firewall policy between a pair of security zones. After you enter this command, you can enter the **service-policy type inspect** command.

If you created only one zone, you can use the system-defined default zone (self) as part of a zone-pair. Such a zone pair and its associated policy applies to traffic directed to the router or generated by the router. It does not affect traffic through the router.

You can specify the **self** keyword for the source or destination, but not for both. You cannot modify or unconfigure the self zone. You can specify the **default** keyword to include all the interfaces that are not configured with any other zones. However, the default zone needs to be defined before it can be used in a zone pair.

Examples

The following example shows how to create zones z1 and z2, identify them, and create a zone pair where z1 is the source and z2 is the destination:

```
zone security z1
 description finance department networks

zone security z2
 description engineering services network

zone-pair security zp source z1 destination z2

zone-pair security
```

The following example shows how to define zone pair z1-z2 and attach the service policy p1 to the zone pair:

```
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
```

The following example shows how the zone pair is configured between system-defined and default zones.

```
zone security default

class-map type inspect match-all tcp-traffic
   match protocol tcp
   match access-group 199

policy-map type inspect p1
   class type inspect tcp-traffic

zone-pair security self-default-zp source self destination default
   service-policy type inspect p1
```

Related Commands

Command	Description
zone-member security	Attaches an interface to a security zone.
zone-pair	Creates a zone pair.