IPv6 Commands: ipv6 a to ipv6 g

ipv6 access-class

To filter incoming and outgoing connections to and from the router based on an IPv6 access list, use the **ipv6 access-class**command in line configuration mode. To disable the filtering of incoming and outgoing connections to the router, use the **no** form of this command.

ipv6 access-class *ipv6-access-list-name* {**in** | **out**}
no ipv6 access-class

Syntax Description

ipv6-access-list-name	Name of an IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
in	Filters incoming IPv6 connections.
out	Filters outgoing IPv6 connections.

Command Default

The filtering of incoming and outgoing connections to and from the router is not enabled.

Command Modes

Line 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The **ipv6 access-class**command is similar to the **access-class** command, except that it is IPv6-specific.

Identical restrictions should be set on all the virtual terminal lines because a user can connect to any of them.

The incoming connection source address is used to match against the access list source prefix. The router address on the received interface is used to match against the access list destination prefix.

IPv6 access control list (ACL) matches are made using TCP; an ACL permit match using IPv6 or TCP is required to allow access to a router.

Examples

The following example filters incoming connections on virtual terminal lines 0 to 4 of the router based on the IPv6 access list named cisco:

```
ipv6 access-list cisco
 permit ipv6 host 2001:0DB8:0:4::2/128 any
line vty 0 4
 ipv6 access-class cisco in
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and sets deny or permit conditions for the defined access list.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name*
no ipv6 access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

Command Default   No IPv6 access list is defined.

Command Modes

Global 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.
12.0(23)S	Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: **permit**, **deny,** *source-ipv6-prefix* / *prefix-length*, **any**, *destination-ipv6-prefix* / *prefix-length*, **priority**. See the "Usage Guidelines" section for more details.
12.2(13)T	Support for IPv6 address configuration mode and extended access list functionality (the filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information) was added. Additionally, the following keywords and arguments were moved from global configuration mode to IPv6 access list configuration mode: **permit**, **deny,** *source-ipv6-prefix* / *prefix-length*, **any**, *destination-ipv6-prefix* / *prefix-length*, **priority**. See the "Usage Guidelines" section for more details.
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	Duplicate remark statements can no longer be configured from the IPv6 access control list.

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

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

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, standard IPv6 access control list (ACL) functionality is used for basic traffic filtering functions--traffic filtering is based on source and destination addresses, inbound and outbound to a specific interface, and with an implicit deny statement at the end of each access list (functionality similar to standard ACLs in IPv4). IPv6 ACLs are defined and their deny and permit conditions are set by using the **ipv6 access-list**command with the **deny** and **permit** keywords in global configuration mode.

In Cisco IOS Release 12.0(23)S or later releases, the standard IPv6 ACL functionality is extended to support--in addition to traffic filtering based on source and destination addresses--filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4). IPv6 ACLs are defined by using the **ipv6 access-list**command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit**commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list**command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

Note   IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

In Cisco IOS Release 12.0(23)S or later releases, and 12.2(11)S or later releases, for backward compatibility, the **ipv6 access-list**command with the **deny** and **permit** keywords in global configuration mode is still supported; however, an IPv6 ACL defined with deny and permit conditions in global configuration mode is translated to IPv6 access list configuration mode.

Refer to the deny (IPv6) and permit (IPv6) commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. See the "Examples" section for an example of a translated IPv6 ACL configuration.

Note   In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

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

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

Note An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

Note When using this command to modify an ACL that is already associated with a bootstrap router (BSR) candidate rendezvous point (RP) (see the **ipv6 pim bsr candidate rp** command) or a static RP (see the **ipv6 pim rp-address** command), any added address ranges that overlap the PIM SSM group address range (FF3x::/96) are ignored. A warning message is generated and the overlapping address ranges are added to the ACL, but they have no effect on the operation of the configured BSR candidate RP or static RP commands.

In Cisco IOS Release 12.2(33)SXH and subsequent Cisco IOS SX releases, duplicate remark statements can no longer be configured from the IPv6 access control list. Because each remark statement is a separate entity, each one is required to be unique.

Examples

The following example is from a device running Cisco IOS Release 12.0(23)S or later releases. The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example is from a device running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S. The example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

If the same configuration was entered on a device running Cisco IOS Release 12.0(23)S or later releases, the configuration would be translated into IPv6 access list configuration mode as follows:

```
ipv6 access-list list2
  deny FEC0:0:0:2::/64 any
  permit ipv6 any any
```

```
interface ethernet 0
 ipv6 traffic-filter list2 out
```

Note   IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Note   IPv6 ACLs defined on a device running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S that rely on the implicit deny condition or specify a **deny any any** statement to filter traffic should contain **permit** statements for link-local and multicast addresses to avoid the filtering of protocol packets (for example, packets associated with the neighbor discovery protocol). Additionally, IPv6 ACLs that use **deny** statements to filter traffic should use a **permit any any** statement as the last statement in the list.

Note   An IPv6 device will not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-class	Filters incoming and outgoing connections to and from the device based on an IPv6 access list.
ipv6 pim bsr candidate rp	Configures the candidate RP to send PIM RP advertisements to the BSR.
ipv6 pim rp-address	Configure the address of a PIM RP for a particular group range.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 access-list log-update threshold

To specify the number of updates that are logged for IPv6 access lists, use the **ipv6 access-list log-update threshold** command in global configuration mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv6 access-list log-update threshold *value*
no ipv6 access-list log-update threshold

Syntax Description

value	Specifies the number of updates that are logged for every IPv6 access list configured on the router. The acceptable range is from 0 to 2147483647.

Command Default

The default is 2147483647 updates.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ipv6 access-list log-update threshold** command is similar to the **ip access-list log-update threshold** command, except that it is IPv6-specific.

IPv6 ACL updates are logged at five minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Examples

The following example configures a log threshold of ten updates for every IPv6 access list configured on the router.

```
ipv6 access-list log-update threshold 10
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

ipv6 address

To configure an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface, use the **ipv6 address**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
no ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

Syntax Description

ipv6-address	The IPv6 address to be used.
/ *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.
prefix-name	A general prefix, which specifies the leading bits of the network to be configured on the interface.
sub-bits	The subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the *prefix-name* argument. The *sub-bits*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default No IPv6 addresses are defined for any interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
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 integrated into Cisco ASR 1000 Series devices.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines	The **ipv6 address** command allows multiple IPv6 addresses to be configured on an interface in various different ways, with varying options. The most common way is to specify the IPv6 address with the prefix length.

Addresses may also be defined using the general prefix mechanism, which separates the aggregated IPv6 prefix bits from the subprefix and host bits. In this case, the leading bits of the address are defined in a general prefix, which is globally configured or learned (for example, through use of Dynamic Host Configuration Protocol-Prefix Delegation (DHCP-PD)), and then applied using the *prefix-name* argument. The subprefix bits and host bits are defined using the *sub-bits* argument.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

IPv6 link-local addresses must be configured and IPv6 processing must be enabled on an interface by using the **ipv6 address link-local** command.

Examples

The following example shows how to enable IPv6 processing on the interface and configure an address based on the general prefix called my-prefix and the directly specified bits:

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

Assuming the general prefix named my-prefix has the value of 2001:DB8:2222::/48, then the interface would be configured with the global address 2001:DB8:2222:7272::72/64.

Related Commands

Command	Description
ipv6 address anycast	Configures an IPv6 anycast address and enables IPv6 processing on an interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 unnumbered	Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.
no ipv6 address autoconfig	Removes all IPv6 addresses from an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 address anycast

To configure an IPv6 anycast address and enable IPv6 processing on an interface, use the **ipv6 address anycast**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix/prefix-length* **anycast**
no ipv6 address [*ip6-prefix/prefix-length* **anycast**]

Syntax Description

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.

Command Default

No IPv6 addresses are defined for any interface.

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.
12.2(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 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

Examples

The following example shows how to enable IPv6 processing on the interface, assign the prefix 2001:0DB8:1:1::/64 to the interface, and configure the IPv6 anycast address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE:

```
ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 anycast
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the 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.

ipv6 address autoconfig

To enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enable IPv6 processing on the interface, use the **ipv6 address autoconfig** command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address autoconfig [**default**]
no ipv6 address autoconfig

Syntax Description

default	(Optional) If a default device is selected on this interface, the **default** keyword causes a default route to be installed using that default device.
	The **default** keyword can be specified only on one interface.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address autoconfig** command causes the device to perform IPv6 stateless address auto-configuration to discover prefixes on the link and then to add the EUI-64 based addresses to the interface. Addresses are configured depending on the prefixes received in Router Advertisement (RA) messages.

Using the **no ipv6 address autoconfig** command without arguments removes all IPv6 addresses from an interface.

Examples

The following example assigns the IPv6 address automatically:

```
Device(config)# interface ethernet 0
Device(config-if)# ipv6 address autoconfig
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the 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.

ipv6 address dhcp

To acquire an IPv6 address on an interface from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp** command in the interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address dhcp [**rapid-commit**]
no ipv6 address dhcp

Syntax Description

rapid-commit	(Optional) Allows the two-message exchange method for address assignment.

Command Default

No IPv6 addresses are acquired from the DHCPv6 server.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 address dhcp** interface configuration command allows any interface to dynamically learn its IPv6 address by using DHCP.

The **rapid-commit** keyword enables the use of the two-message exchange for address allocation and other configuration. If it is enabled, the client includes the rapid-commit option in a solicit message.

Examples

The following example shows how to acquire an IPv6 address and enable the rapid-commit option:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp
rapid-commit
```

You can verify your settings by using the **show ipv6 dhcp interface** command in privileged EXEC mode.

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCPv6 interface information.

ipv6 address dhcp client request

To configure an IPv6 client to request a vendor-specific option from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server, use the **ipv6 address dhcp client request** command in interface configuration mode. To remove the request, use the **no** form of this command.

ipv6 address dhcp client request vendor

no ipv6 address dhcp client request vendor

Syntax Description

vendor	Requests the vendor-specific options.

Command Default

IPv6 clients are not configured to request an option from DHCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **ipv6 address dhcp client request vendor** command to request a vendor-specific option. When this command is enabled, the IPv6 client can request a vendor-specific option only when an IPv6 address is acquired from DHCP. If you enter the command after the interface has acquired an IPv6 address, the IPv6 client cannot request a vendor-specific option until the next time the client acquires an IPv6 address from DHCP.

Examples

The following example shows how to configure an interface to request vendor-specific options:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ipv6 address dhcp client request vendor
```

Related Commands

Command	Description
ipv6 address dhcp	Acquires an IPv6 address on an interface from the DHCPv6 server.

ipv6 address eui-64

To configure an IPv6 address for an interface and enables IPv6 processing on the interface using an EUI-64 interface ID in the low order 64 bits of the address, use the **ipv6 address eui-64**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-prefix/prefix-length* **eui-64**
no ipv6 address [*ip v6-prefix/prefix-length* **eui-64**]

Syntax Description

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.

Command Default   No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines   If the value specified for the / *prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID.

Using the no ipv6 address command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco IOS software detects another host using one of its IPv6 addresses, it will display an error message on the console.

Examples

The following example assigns IPv6 address 2001:0DB8:0:1::/64 to Ethernet interface 0 and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
Router(config)# interface ethernet 0
Router(config-if)# ipv6 address 2001:0DB8:0:1::/64 eui-64
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the 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.

ipv6 address link-local

To configure an IPv6 link-local address for an interface and enable IPv6 processing on the interface, use the **ipv6 address link-local**command in interface configuration mode. To remove the address from the interface, use the **no** form of this command.

ipv6 address *ipv6-address/prefix-length* **link-local** [**cga**]
no ipv6 address [*ipv6-address/prefix-length* **link-local**]

Syntax Description

ipv6-address	The IPv6 address 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	Specifies a link-local address. The *ipv6-address* specified with this command overrides the link-local address that is automatically generated for the interface.
cga	(Optional) Specifies the CGA interface identifier.

Command Default

No IPv6 address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(24)T	The **cga** keyword was added
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines	Using the **no ipv6 address** command without arguments removes all manually configured IPv6 addresses from an interface.

If the Cisco software detects another host using one of its IPv6 addresses, it will display an error message on the console.

The system automatically generates a link-local address for an interface when IPv6 processing is enabled on the interface, typically when an IPv6 address is configured on the interface. To manually specify a link-local address to be used by an interface, use the ipv6 address link-local command.

A double colon may be used as part of the *ipv6-address* argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

Examples

The following example assigns FE80::260:3EFF:FE11:6770 as the link-local address for Ethernet interface 0:

```
interface ethernet 0
 ipv6 address FE80::260:3EFF:FE11:6770 link-local
```

Related Commands

Command	Description
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
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.

ipv6 atm-vc

To configure a mapping between a virtual circuit (VC) and the IPv6 address of a system at the far end of that circuit, use the **ipv6 atm-vc** command in map-list configuration mode. To remove the mapping, use the **no** form of this command.

ipv6 *ipv6-address* **atm-vc** *vcd* [**broadcast**]
no ipv6 *ipv6-address* **atm-vc** *vcd* [**broadcast**]

Syntax Description

ipv6-address	The IPv6 address of a system at the far end of the specified virtual circuit.
	This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
vcd	The virtual circuit descriptor for the virtual circuit mapped to the specified IPv6 address.
broadcast	(Optional) Specifies that this map entry is used when sending IPv6 multicast packets to the interface (for example, network routing protocol updates).

Command Default

No default behavior or values.

Command Modes

Map-list 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

ATM permanent virtual circuits (PVCs) can be configured in the following modes:

- Nonbroadcast multiaccess (NBMA) mode--A neighbor is mapped to a PVC. ATM point-to-multipoint PVCs are configured using static maps. The ipv6 atm-vc command utilizes static maps.

- Point-to point-mode--Each PVC is given a subinterface and is configured as a standard point-to-point link.

Note   We recommend configuring ATM PVCs in point-to-point mode.

Examples

The following example maps neighbor 2001:0DB8::5 to ATM point-to-multipoint PVC 1, virtual path identifier (VPI) 3, and virtual channel identifier (VCI) 5:

```
Router(config)# interface atm 1/0
Router(config-if)# atm pvc 1 3 5 aal5snap
Router(config-if)# map-group cisco
Router(config)# map-list cisco
Router(config-map-list)# ipv6 2001:0DB8::5 atm-vc 1
```

Related Commands

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

ipv6 authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets, use the **ipv6 authentication key-chain eigrp**command in interface configuration mode. To disable authentication of EIGRP for IPv6 packets, use the **no** form of this command.

ipv6 authentication key-chain eigrp *as-number* *key-chain*
no ipv6 authentication key-chain eigrp *as-number* *key-chain*

Syntax Description

as-number	Autonomous system number.
key-chain	Name of the authentication key chain.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 route authentication provides Message Digest 5 (MD5) authentication of routing updates from the EIGRP for IPv6 routing protocol. The MD5 keyed digest in each EIGRP for IPv6 packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters.

Examples

The following example enables authentication for EIGRP for IPv6 for AS 1, using a key chain named chain1:

```
Router(config-if)# ipv6 authentication key-chain eigrp 1 chain1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.

Command	Description
ipv6 authentication mode eigrp	Specifies the type of authentication used in EIGRP for IPv6 packets.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets for IPv6, use the **ipv6 authentication mode eigrp**command in interface configuration mode. To disable the type of authentication, use the **no** form of this command.

ipv6 authentication mode eigrp *as-number* **md5**
no ipv6 authentication mode eigrp *as-number* **md5**

Syntax Description

as-number	Autonomous system number.
md5	Specifies keyed message digest 5 (MD5) authentication.

Command Default

No authentication is provided for EIGRP for IPv6 packets.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Use the **ipv6 authentication mode eigrp**command to configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP for IPv6 packet in the specified autonomous system.

Examples

The following example configures the interface to use MD5 authentication in EIGRP for IPv6 packets in autonomous system 1:

```
Router(config-if)# ipv6 authentication mode eigrp 1 md5
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
ipv6 authentication key-chain eigrp	Enables authentication of EIGRP packets for IPv6.
key	Identifies an authentication key on a key chain.
key chain	Enables authentication of routing protocols.
key-string (authentication)	Specifies the authentication string for a key.

Command	Description
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

ipv6 bandwidth-percent eigrp

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on an interface, use the **ipv6 bandwidth-percent eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 bandwidth-percent eigrp *as-number percent*
no ipv6 bandwidth-percent eigrp *as-number percent*

Syntax Description

as-number	Autonomous system number.
percent	Percentage of bandwidth that EIGRP for IPv6 may use.

Command Default

Percentage of bandwidth used is 50 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

EIGRP for IPv6 uses as much as 50 percent of the bandwidth of a link, as defined by the **bandwidth** command. The ipv6 bandwidth-percent eigrp command may be used if some other fraction of the bandwidth is desired.

Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

Examples

The following example allows EIGRP for IPv6 to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 1:

```
interface serial 0
 bandwidth 56
 ipv6 bandwidth-percent eigrp 1 75
```

Related Commands

Command	Description
bandwidth (interface)	Sets a bandwidth value for an interface.

ipv6 cef

To enable Cisco Express Forwarding for IPv6, use the **ipv6 cef** command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef
no ipv6 cef

Syntax Description This command has no arguments or keywords.

Command Default Cisco Express Forwarding for IPv6 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines The **ipv6 cef** command is similar to the **ip cef** command, except that it is IPv6-specific.

The **ipv6 cef** command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed Cisco Express Forwarding for IPv6 mode.

Note The **ipv6 cef**command is not supported in interface configuration mode.

Note Some distributed architecture platforms, such as the Cisco 7500 series routers, support both Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6. When Cisco Express Forwarding for IPv6 is configured on distributed platforms, Cisco Express Forwarding switching is performed by the Route Processor (RP).

✎

| **Note** | You must enable Cisco Express Forwarding for IPv4 by using the **ip cef** global configuration command before enabling Cisco Express Forwarding for IPv6 by using the **ipv6 cef** global configuration command. |

Cisco Express Forwarding for IPv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as Cisco Express Forwarding for IPv4. Cisco Express Forwarding for IPv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples

The following example enables standard Cisco Express Forwarding for IPv4 operation and then standard Cisco Express Forwarding for IPv6 operation globally on the router.

```
ip cef
ipv6 cef
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
ipv6 cef accounting	Enables Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting.
ipv6 cef distributed	Enables distributed Cisco Express Forwarding for IPv6.
show cef	Displays which packets the line cards dropped or displays which packets were not express-forwarded.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef accounting

To enable Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting, use the **ipv6 cef accounting**command in global configuration mode or interface configuration mode. To disable Cisco Express Forwarding for IPv6 network accounting, use the **no**form of this command.

ipv6 cef accounting *accounting-types*
no ipv6 cef accounting *accounting-types*

Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode
ipv6 cef accounting non-recursive {**external** | **internal**}
no ipv6 cef accounting non-recursive {**external** | **internal**}

Syntax Description

accounting-types	The *accounting-types* argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once. • **load-balance-hash** --Enables load balancing hash bucket counters. • **non-recursive** --Enables accounting through nonrecursive prefixes. • **per-prefix** --Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix). • **prefix-length** --Enables accounting through prefix length.
non-recursive	Enables accounting through nonrecursive prefixes. This keyword is optional when used in global configuration mode after another keyword is entered. See the *accounting-types* argument.
external	Counts input traffic in the nonrecursive external bin.
internal	Counts input traffic in the nonrecursive internal bin.

Command Default

Cisco Express Forwarding for IPv6 network accounting is disabled by default.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **non-recursive**and **load-balance-hash**keywords were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

Configuring Cisco Express Forwarding for IPv6 network accounting enables you to collect statistics on Cisco Express Forwarding for IPv6 traffic patterns in your network.

When you enable network accounting for Cisco Express Forwarding for IPv6 by using the **ipv6 cef accounting**command in global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding for IPv6 mode is enabled and at the line cards when distributed Cisco Express Forwarding for IPv6 mode is enabled. You can then display the collected accounting information using the **show ipv6 cef** EXEC command.

For prefixes with directly connected next hops, the **non-recursive** keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode after you enter another keyword on the **ipv6 cef accounting**command.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the **show ipv6 cef detail**command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the **load-balance-hash** keyword with the **ipv6 cef accounting** command to enable per-hash-bucket counters. Enter the **show ipv6 cef** *prefix* **internal** command to display the per-hash-bucket counters.

Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Router(config)# ipv6 cef accounting non-recursive
```

Related Commands

Command	Description
ip cef accounting	Enable Cisco Express Forwarding network accounting (for IPv4).
show cef	Displays information about packets **forwarded by Cisco Express Forwarding.**

Command	Description
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6, use the **ipv6 cef distributed**command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the **no** form of this command.

ipv6 cef distributed
no ipv6 cef distributed

Syntax Description   This command has no arguments or keywords.

Command Default   Distributed Cisco Express Forwarding for IPv6 is disabled on the Cisco 7500 series routers and enabled on the Cisco 12000 series Internet routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(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 implemented on Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines   The **ipv6 cef distributed**command is similar to the **ip cef distributed**command, except that it is IPv6-specific.

Enabling distributed Cisco Express Forwarding for IPv6 globally on the router by using the **ipv6 cef distributed**in global configuration mode distributes the Cisco Express Forwarding processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.

Note   The **ipv6 cef distributed** command is not supported on the Cisco 12000 series Internet routers because distributed Cisco Express Forwarding for IPv6 is enabled by default on this platform.

Note To forward distributed Cisco Express Forwarding for IPv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the **ipv6 unicast-routing** global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the **ipv6 address** interface configuration command.

Note You must enable distributed Cisco Express Forwarding for IPv4 by using the **ip cef distributed**global configuration command before enabling distributed Cisco Express Forwarding for IPv6 by using the **ipv6 cef distributed**global configuration command.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

Examples The following example enables distributed Cisco Express Forwarding for IPv6 operation:

```
ipv6 cef distributed
```

Related Commands

Command	Description
ip route-cache	Controls the use of high-speed switching caches for IP routing.
show ipv6 cef	Displays entries in the IPv6 FIB.

ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the **ipv6 cef load-sharing algorithm** command in global configuration mode. To return to the default universal load-balancing algorithm, use the **no** form of this command.

ipv6 cef load-sharing algorithm {**original** | **universal** [*id*] | **include-ports** {**source** [*id*] | [**destination**] [*id*] | **source** [*id*] **destination** [*id*] **gtp**}}
no ipv6 cef load-sharing algorithm

Syntax Description

original	Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
universal	Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
id	(Optional) Fixed identifier in hexadecimal format.
include-ports source	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 source port.
include-ports destination	Sets the load-balancing algorithm to the include-ports algorithm that uses a Layer 4 destination port.
include-ports source destination	Sets the load balancing algorithm to the include-ports algorithm that uses Layer 4 source and destination ports.
include-ports source destination gtp	Sets the load-balancing algorithm based on the GPRS Tunneling Protocol Tunnel Endpoint Identifier (GTP TEID) for the GTP-U packets. Sets the load-balancing algorithm based on the Layer 4 source and destination ports for the non-GTP-U packets.

Command Default

The universal load-balancing algorithm is selected. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
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.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
3.10S	This command is supported in Cisco IOS XE Release 3.10S. The **gtp** keyword was added to the command.

Usage Guidelines

The **ipv6 cef load-sharing algorithm**command is similar to the **ip cef load-sharing algorithm**command, except that it is IPv6-specific.

When the Cisco Express Forwarding for IPv6 load-balancing algorithm is set to universal mode, each router on the network can make a different load-sharing decision for each source-destination address pair.

The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal-cost paths that are not load-shared because the majority of the traffic is between peer addresses that use different port numbers, such as Real-Time Protocol (RTP) streams.

Examples

The following example shows how to enable the Cisco Express Forwarding load-balancing algorithm for IPv6 for Layer-4 source and destination ports:

```
Router(config)# ipv6 cef load-sharing algorithm include-ports source destination
```

The router automatically generates fixed IDs for the algorithm.

The following example shows how to enable the IPv6 CEF load-sharing algorithm based on GTP TEID:

```
configure terminal
!
 ipv6 cef load-sharing algorithm include-ports source destination gtp
 exit
```

Related Commands

Command	Description
debug ipv6 cef hash	Displays debug messages for Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 load-sharing hash algorithm events.
ip cef load-sharing algorithm	Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).

ipv6 cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **ipv6 cef optimize neighbor resolution**command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the **no** form of this command.

ipv6 cef optimize neighbor resolution
no ipv6 cef optimize neighbor resolution

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, Cisco Express Forwarding for IPv6 does not optimize the address resolution of directly connected neighbors.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

The **ipv6 cef optimize neighbor resolution** command is very similar to the **ip cef optimize neighbor resolution** command, except that it is IPv6-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv6.

Examples

The following example shows how to optimize address resolution from Cisco Express Forwarding for IPv6 for directly connected neighbors:

```
Router(config)# ipv6 cef optimize neighbor resolution
```

Related Commands

Command	Description
ip cef optimize neighbor resolution	Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.

ipv6 cga modifier rsakeypair

To generate an IPv6 cryptographically generated address (CGA) modifier for a specified Rivest, Shamir, and Adelman (RSA) key pair, use the **ipv6 cga modifier rsakeypair**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga modifier rsakeypair *key-label* **sec-level** *sec-level-value* [{**max-iterations value** *cga-modifier*}]
no ipv6 cga modifier rsakeypair

Syntax Description		
key-label	The name to be used for RSA key pair
sec-level *sec-level-value*	Specifies the security level, which can be a number from 0 through 3. The most secure level is 1.
max-iterations*value*	(Optional) Maximum iteration for modifier generation. The *value* can be a number from 0 through 40000000.
cga-modifier	(Optional) An IPv6 address used as a CGA modifier.

Command Default

No CGA exists for an RSA key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(3)T	The **max-iterations** keyword and *cga-modifier* argument were added.

Usage Guidelines

Use this command to generate the CGA modifier for a specified RSA key pair, which enables the key to be used by Secure Neighbor Discovery (SeND).

Once the RSA key is generated, the modifier must be generated as well, using the **ipv6 cga modifier rsakeypair** command.

A CGA has a security parameter that determines its strength against brute-force attacks. The security level can be either 0 or 1.

Examples

The following example enables the specified key to be used by SeND (that is, generates the modifier):

```
Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair	Generates the CGA modifier for a specified RSA key.

Command	Description
ipv6 cga modifier rsakeypair (interface)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 cga rsakeypair

To bind a Secure Neighbor Discovery (SeND) key to a specified interface, use the **ipv6 cga rsakeypair**command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga rsakeypair *key-label*
no ipv6 cga rsakeypair

Syntax Description	*key-label*	The name to be used for the Rivest, Shamir, and Adelman (RSA) key pair.

Command Default A SeND key is not bound to an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines The SeND key is used to generate an IPv6 modifier for a specified Rivest, Shamir and Adelman (RSA) key pair. A SeND key must be bound to the interface prior to its being used in the **ipv6 address** command. Use the **ipv6 cga rsakeypair** command to bind a SeND key to a specified interface.

You can then use the **ipv6 address** command to add the Cryptographic Addresses (CGA).

Examples The following example binds a SeND key to Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.1.1 255.255.255.0
Router(config-if)# ipv6 cga rsakeypair SEND
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair (global configuration)	Generates the CGA modifier for a specified RSA key.
ipv6 cga modifier rsakeypair (interface configuration)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 crypto map

To enable an IPv6 crypto map on an interface, use the **ipv6 crypto map** command in interface configuration mode. To disable, use the **no** form of this command.

ipv6 crypto map *map-name*
no ipv6 crypto map

Syntax Description

map-name	Identifies the crypto map set.

Command Default

No IPv6 crypto maps are enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command differentiates IPv6 and IPv4 crypto maps.

Examples

The following example shows how to enable an IPv6 crypto map on an interface:

```
Router# configure terminal
Router(config
)# interface ethernet 0/0
Router(config-if
)# ipv6 crypto map CM_V4
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry.

ipv6 destination-guard attach-policy

To attach a destination guard policy, use the **ipv6 destination-guard attach-policy** command in VLAN configuration mode or interface configuration mode. To unattach the destination-guard policy, use the **no** form of this command.

ipv6 destination-guard attach-policy [*policy-name*]
no ipv6 destination-guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of the destination guard policy.

Command Default   No destination guard policy is attached.

Command Modes   VLAN configuration (config-vlan-config)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines   This command allows you to attach a destination guard policy to a router or an interface. These policies can be used to filter IPv6 traffic based on the destination address, and block any data traffic from an unknown source.

Examples   The following example shows how to attach a destination guard policy to a router:

```
Device> enable
Device# configure terminal
Device(config)# vlan configuration 1
Device(config-vlan-config)# ipv6 destination-guard attach-policy pol1
```

Related Commands

Command	Description
ipv6 destination-guard policy	Defines the destination guard policy.
show ipv6 destination-guard policy	Displays destination guard information.

ipv6 destination-guard policy

To define a destination guard policy, use the **ipv6 destination-guard policy** command in global configuration mode. To remove the destination guard policy, use the **no** form of this command.

ipv6 destination-guard policy [*policy-name*]
no ipv6 destination-guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of the destination guard policy.

Command Default   No destination guard policy is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines   This command enters destination-guard configuration mode. The destination guard policies can be used to filter IPv6 traffic based on the destination address to block data traffic from an unknown source.

Examples   The following example shows how to define the name of a destination guard policy:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 destination-guard policy policy1
Router(config-destguard)#
```

Related Commands

Command	Description
show ipv6 destination-guard policy	Displays destination guard information.

ipv6 dhcp binding track ppp

To configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to release any bindings associated with a PPP connection when that connection closes, use the **ipv6 dhcp binding track ppp** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp

Syntax Description

This command has no arguments or keywords.

Command Default

When a PPP connection closes, the DHCP bindings associated with that connection are not released.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

The **ipv6 dhcp binding track ppp** command configures DHCP for IPv6 to automatically release any bindings associated with a PPP connection when that connection is closed. The bindings are released automatically to accommodate subsequent new registrations by providing sufficient resource.

Note In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using this command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

A binding table entry on the DHCP for IPv6 server is automatically:

• Created whenever a prefix is delegated to a client from the configuration pool.

• Updated when the client renews, rebinds, or confirms the prefix delegation.

• Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or an administrator clears the binding.

Examples

The following example shows how to release the prefix bindings associated with the PPP:

```
Router(config)# ipv6 dhcp binding track ppp
```

ipv6 dhcp client information refresh minimum

To configure the minimum acceptable Dynamic Host Configuration Protocol (DHCP) for IPv6 client information refresh time on a specified interface, use the **ipv6 dhcp client information refresh minimum**command in interface configuration mode. To remove the configured refresh time, use the **no** form of this command.

ipv6 dhcp client information refresh minimum *seconds*
no ipv6 dhcp client information refresh minimum *seconds*

Syntax Description

seconds	The refresh time, in seconds. The minimum value that can be used is 600 seconds.

Command Default   The default is 86,400 seconds (24 hours).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines   The **ipv6 dhcp client information refresh minimum**command specifies the minimum acceptable information refresh time. If the server sends an information refresh time option of less than the configured minimum refresh time, the configured minimum refresh time will be used instead.

This command may be configured in several situations:

- In unstable environments where unexpected changes are likely to occur.

- For planned changes, including renumbering. An administrator can gradually decrease the time as the planned event nears.

- Limit the amount of time before new services or servers are available to the client, such as the addition of a new Simple Network Time Protocol (SNTP) server or a change of address of a Domain Name System (DNS) server.

Examples   The following example configures an upper limit of 2 hours:

```
ipv6 dhcp client information refresh minimum 7200
```

ipv6 dhcp client pd

To enable the Dynamic Host Configuration Protocol (DHCP) for IPv6 client process and enable request for prefix delegation through a specified interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable requests for prefix delegation, use the **no** form of this command.

ipv6 dhcp client pd {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]
no ipv6 dhcp client pd

Syntax Description		
prefix-name	IPv6 general prefix name.
hint	An IPv6 prefix sent as a hint.
ipv6-prefix	IPv6 general prefix.
rapid-commit	(Optional) Allow two-message exchange method for prefix delegation.

Command Default

Prefix delegation is disabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Enabling the **ipv6 dhcp client pd**command starts the DHCP for IPv6 client process if this process is not yet running.

The **ipv6 dhcp client pd**command enables request for prefix delegation through the interface on which this command is configured. When prefix delegation is enabled and a prefix is successfully acquired, the prefix is stored in the IPv6 general prefix pool with an internal name defined by the *ipv6-prefix*argument. Other commands and applications (such as the **ipv6 address** command) can then refer to the prefixes in the general prefix pool.

The **hint** keyword with the *ipv6-prefix* argument enables the configuration of an IPv6 prefix that will be included in DHCP for IPv6 solicit and request messages sent by the DHCP for IPv6 client on the interface as a hint to prefix-delegating routers. Multiple prefixes can be configured by issuing the **ipv6 dhcp client pd hint***ipv6-prefix* command multiple times. The new prefixes will not overwrite old ones.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If it is enabled, the client will include the rapid commit option in a solicit message.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

Examples

The following example enables prefix delegation:

```
Router(config-if)# ipv6 dhcp client pd dhcp-prefix
```

The following example configures a hint for prefix-delegating routers:

```
Router(config-if)# ipv6 dhcp client pd hint 2001:0DB8:1/48
```

Related Commands

Command	Description
clear ipv6 dhcp client	Restarts the DHCP for IPv6 client on an interface.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp client vendor-class

The DHCPv6 client, by default, carries the PID (product ID) of the device in option-16. To override this behaviour, use the following command:

ipv6   dhcp   client   vendor-class   [{ **mac-address** | **ascii** | **hex** | **disable** }]

Syntax Description

mac-address	The MAC address of the device.
ascii	The user defined string in ASCII format.
hex	The user defined string in hexadecimal format.
disable	Disables sending option 16 in DHCPv6 messages.

Command Default

By default, option 16 is enabled and the DHCPv6 client carries the PID (Product ID) of device.

Command Modes

Interface configuration mode.

Usage Guidelines

By default DHCPv6 client carries PID of the device in option-16. This default behaviour can be overridden by configuring the **ipv6 dhcp client vendor-class** command.

Examples

The following example enables option-16:

```
Router(config-if)# ipv6 dhcp client ?
information Configure information refresh option
pd Prefix-Delegation
request Request
vendor-class Configure vendor class data, Product ID by default (Option 16)
```

The following configuration example overrides PID with mac-address:

```
Router(config-if)# ipv6 dhcp client vendor-class mac-address
```

Examples

The following configuration example overrides PID with user defined string in the hex format:

```
Router(config-if)# ipv6 dhcp client vendor-class hex aabbcc
```

Examples

The following configuration example overrides PID with user defined string in the ascii format:

```
Router(config-if)# ipv6 dhcp client vendor-class ascii cisco
```

Examples

The following configuration example is used to disable sending option-16 in DHCPv6 messages:

```
Router(config-if)# ipv6 dhcp client vendor-class disable
```

ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the **ipv6 dhcp database** command in global configuration mode. To delete the database agent, use the **no** form of this command.

ipv6 dhcp database *agent* [**write-delay** *seconds*] [**timeout** *seconds*]
no ipv6 dhcp database *agent*

Syntax Description

agent	A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy Protocol (RCP) uniform resource locator.
write-delay *seconds*	(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The default is 300 seconds. The minimum write delay is 60 seconds.
timeout *seconds*	(Optional) How long, in seconds, the router waits for a database transfer.

Command Default

Write-delay default is 300 seconds. Timeout default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **ipv6 dhcp database** command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, updated when the client renews, rebinds, or confirms the prefix delegation, and deleted when the client releases all the prefixes in the binding voluntarily, all prefixes' valid lifetimes have expired, or administrators enable the clear ipv6 dhcp binding command. These bindings are maintained in RAM and can be saved to permanent storage using the *agent* argument so that the information about configuration such as prefixes assigned to clients is not lost after a system reload or power down. The bindings are stored as text records for easy maintenance.

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host such as an FTP server or a local file system such as NVRAM.

The **write-delay** keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The **timeout** keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are terminated. By default, the DHCP for IPv6 server waits 300 seconds before terminating a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

Examples   The following example specifies DHCP for IPv6 binding database agent parameters and stores
binding entries in TFTP:

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding
```

The following example specifies DHCP for IPv6 binding database agent parameters and stores
binding entries in bootflash:

```
ipv6 dhcp database bootflash
```

Related Commands

Command	Description
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 server binding table
show ipv6 dhcp database	Displays DHCP for IPv6 binding database agent information.

ipv6 dhcp debug redundancy

To display debugging output for IPv6 DHCP high availability (HA) processing, use the **ipv6 dhcp debug redundancy**command in privileged EXEC mode. To disable debugging output, use the no form of this command.

ipv6 dhcp debug redundancy
no ipv6 dhcp debug redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **ipv6 dhcp debug redundancy** command to display stateful switchover (SSO) state transitions and errors.

Examples

The following example enables IPv6 DHCP redundancy debugging:

```
Router# ipv6 dhcp debug redundancy
```

ipv6 dhcp framed password

To assign a framed prefix when using a RADIUS server, use the **ipv6 dhcp framed password**command in interface configuration mode. To remove the framed prefix, use the **no** form of this command.

ipv6 dhcp framed password *password*
no ipv6 dhcp framed password

Syntax Description

password	Password to be used with the RADIUS server.

Command Default   No framed prefix is assigned.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines   The ipv6 dhcp framed password command enables a user to request a framed prefix of a RADIUS server. When a PPPoE client requests a prefix from a network using the framed-prefix system, the RADIUS server should assign an address. However, the RADIUS server is configured to receive a password. Because the client does not send a password, the RADIUS server does not send a framed prefix.

> **Note**   Ordinarily, the **ipv6 dhcp framed password** command will not need to be used because a client will have been authenticated as part of PPP session establishment.

Examples   The following example shows how to configure a password to be used with the RADIUS server:

```
Router(config-if)# ipv6 dhcp framed password password1
```

ipv6 dhcp guard attach-policy

To attach a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy, use the **ipv6 dhcp guard attach-policy** command in interface configuration or VLAN configuration mode. To unattach the DHCPv6 guard policy, use the **no** form of this command.

Syntax Available In Interface Configuration Mode
ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [. . . *vlan-id*]]
no ipv6 dhcp guard [**attach-policy** [*policy-name*]] [**vlan** {**add** | **all** | **except** | **none** | **remove**} *vlan-id* [. . . *vlan-id*]]

Syntax Available In VLAN Configuration Mode
ipv6 dhcp guard attach-policy [*policy-name*]
no ipv6 dhcp guard attach-policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.
vlan	(Optional) Specifies that the DHCPv6 policy is to be attached to a VLAN.
add	(Optional) Attaches a DHCPv6 guard policy to the specified VLAN(s).
all	(Optional) Attaches a DHCPv6 guard policy to all VLANs.
except	(Optional) Attaches a DHCPv6 guard policy to all VLANs except the specified VLAN(s).
none	(Optional) Attaches a DHCPv6 guard policy to none of the specified VLAN(s).
remove	(Optional) Removes a DHCPv6 guard policy from the specified VLAN(s).
vlan-id	(Optional) Identity of the VLAN(s) to which the DHCP guard policy applies.

Command Default   No DHCPv6 guard policy is attached.

Command Modes   Interface configuration (config-if)

VLAN configuration (config-vlan)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines   This command allows you to attach a DHCPv6 policy to an interface or to one or more VLANs. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to attach a DHCPv6 guard policy to an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet 0/2/0
Router# switchport
Router(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp guard policy

To define a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy name, use the **ipv6 dhcp guard policy** command in global configuration mode. To remove the DHCPv6 guard policy name, use the **no** form of this command.

ipv6 dhcp guard policy [*policy-name*]
no ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Default   No DHCPv6 guard policy name is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines   This command allows you to enter DHCPv6 guard configuration mode. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples   The following example shows how to define a DHCPv6 guard policy name:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp guard policy policy1
```

Related Commands

Command	Description
show ipv6 dhcp guard policy	Displays DHCPv6 guard policy information.

ipv6 dhcp ping packets

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the **ipv6 dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

ipv6 dhcp ping packets *number*
ipv6 dhcp ping packets

Syntax Description	*number*	The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10.

Command Default   No ping packets are sent before the address is assigned to a requesting client.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines   The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to 0 turns off the DHCPv6 server ping operation

Examples   The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Router(config)# ipv6 dhcp ping packets 4
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.
show ipv6 dhcp conflict	Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.

ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the **ipv6 dhcp pool** command in global configuration mode. To delete a DHCP for IPv6 pool, use the **no** form of this command.

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).

Command Default   DHCP for IPv6 pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines   Use the **ipv6 dhcp pool**command to create a DHCP for IPv6 server configuration information pool. When the **ipv6 dhcp pool** command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.

- **link-address** *IPv6-prefix* sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.

- **vendor-specific** *vendor-id* enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:

  - **suboption** *number* sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

Note   The **hex** value used under the **suboption** keyword allows users to enter only hex digits (0-f). Entering an invalid **hex** value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the **ipv6 dhcp server** command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the **ipv6 dhcp server interface** configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The **link-address** command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

Examples   The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

Related Commands

Command	Description
ipv6 dhcp server	Enables DHCP for IPv6 service on an interface.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

ipv6 dhcp relay destination

To specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface, use the **ipv6 dhcp relay destination** command in interface configuration mode. To remove a relay destination on the interface or to delete an output interface for a destination, use the **no** form of this command.

ipv6 dhcp relay destination *ipv6-address* [{*interface-type interface-number* | **vrf** *vrf-name* | **global**}]
no ipv6 dhcp relay destination *ipv6-address* [{*interface-type interface-number* | **vrf** *vrf-name* | **global**}]

Cisco CMTS Routers

ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address***source-address*]
no ipv6 dhcp relay destination *ipv6-address* [*interface-type interface-number*] [**link-address** *link-address*] [**source-address** *source-address*]

Syntax Description		
	ipv6-address	Relay destination address. There are two types of relay destination address: • Link-scoped unicast or multicast IPv6 address. A user must specify an output interface for this kind of address. • Global or site-scoped unicast or multicast IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
	interface-type interface-number	(Optional) Interface type and number that specifies the output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.
	vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) associated with the relay destination IPv6 address.
	global	(Optional) Specifies the relay destination when the relay destination is in the global address space and when the relay source is in a VRF.
	link-address *link-address*	(Optional) Specifies the DHCPv6 link address. The link-address must be an IPv6 globally scoped address configured on the network interface where the DHCPv6 relay is operational.
	source-address *source-address*	(Optional) Specifies the Cisco CMTS network interface source address. The source-address can be any IPv6 global-scoped address on the router.

Command Default   The relay function is disabled, and there is no relay destination on an interface.

Command Modes

Interface configuration (config-if)

Command History	Release	Modification
	12.3(11)T	This command was introduced.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
	12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
	15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added. The **global** keyword was added.
	Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
	12.2(33)SCE5	This command was integrated into Cisco IOS Release 12.2(33)SCE5. The **link-address** and **source-address** keywords were added.
	15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

The **ipv6 dhcp relay destination** command specifies a destination address to which client messages are forwarded, and it enables DHCP for IPv6 relay service on the interface. When relay service is enabled on an interface, a DHCP for IPv6 message received on that interface will be forwarded to all configured relay destinations. The incoming DHCP for IPv6 message may have come from a client on that interface, or it may have been relayed by another relay agent.

The relay destination can be a unicast address of a server or another relay agent, or it may be a multicast address. There are two types of relay destination addresses:

- A link-scoped unicast or multicast IPv6 address, for which a user must specify an output interface

- A global or site-scoped unicast or multicast IPv6 address. A user can optionally specify an output interface for this kind of address.

If no output interface is configured for a destination, the output interface is determined by routing tables. In this case, it is recommended that a unicast or multicast routing protocol be running on the router.

Multiple destinations can be configured on one interface, and multiple output interfaces can be configured for one destination. When the relay agent relays messages to a multicast address, it sets the hop limit field in the IPv6 packet header to 32.

Unspecified, loopback, and node-local multicast addresses are not acceptable as the relay destination. If any one of them is configured, the message "Invalid destination address" is displayed.

Note that it is not necessary to enable the relay function on an interface for it to accept and forward an incoming relay reply message from servers. By default, the relay function is disabled, and there is no relay destination on an interface. The **no** form of the command removes a relay destination on an interface or deletes an output interface for a destination. If all relay destinations are removed, the relay service is disabled on the interface.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

In Cisco CMTS, if you change one or more parameters of this command, you have to disable the command using the no form, and execute the command again with changed parameters.

The default behavior (when **no source-address**, **link-address**, and **no output interface** commands are provisioned in the **ipv6 dhcp relay destination** command) of the new functionality is to copy the Cisco IOS SAS-computed source address to the link-address of the DHCPv6 relay-forward message.

Examples

The following example sets the relay destination address on Ethernet interface 4/3:

```
ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3
```

The following example shows how to set the relay destination address on the Ethernet interface 4/3 on a Cisco CMTS router:

```
ipv6 dhcp relay destination 2001:db8:1234:5678:9abc:def1:2345:6789 ethernet 4/3
```

Related Commands

Command	Description
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the ipv6 dhcp-relay option vpn command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn

Syntax Description   This command has no arguments or keywords.

Command Default   The DHCP for IPv6 relay VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines   The **ipv6 dhcp-relay option vpn** command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the router. If the **ipv6 dhcp relay option vpn** command is enabled on a specified interface, it overrides the global **ipv6 dhcp-relay option vpn** command.

Examples   The following example enables the DHCPv6 relay VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp-relay option vpn
```

Related Commands

Command	Description
ipv6 dhcp relay option vpn	Enables the DHCPv6 relay VRF-aware feature on an interface.

ipv6 dhcp relay source-interface

To configure an interface to use as the source when relaying messages received on this interface, use the **ipv6 dhcp relay source-interface**command in interface configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp relay source-interface *type number*
no ipv6 dhcp relay source-interface *type number*

Syntax Description	*type number*	Interface type and number that specifies output interface for a destination. If these arguments are configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config-if)# ipv6 dhcp relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp-relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp-relay bulk-lease

To configure bulk lease query parameters, use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode. To remove the bulk-lease query configuration, use the **no** form of this command.

ipv6 dhcp-relay bulk-lease {**data-timeout** *seconds* | **retry** *number*} [**disable**]
no ipv6 dhcp-relay bulk-lease [**disable**]

Syntax Description

data-timeout	(Optional) Bulk lease query data transfer timeout.
seconds	(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.
retry	(Optional) Sets the bulk lease query retries.
number	(Optional) The range is from 0 to 5. The default is 5.
disable	(Optional) Disables the DHCPv6 bulk lease query feature.

Command Default

Bulk lease query is enabled automatically when the DHCP for IPv6 (DHCPv6) relay agent feature is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.

Usage Guidelines

Use the **ipv6 dhcp-relay bulk-lease**command in global configuration mode to configure bulk lease query parameters, such as data transfer timeout and bulk-lease TCP connection retries.

The DHCPv6 bulk lease query feature is enabled automatically when the DHCPv6 relay agent is enabled. The DHCPv6 bulk lease query feature itself cannot be enabled using this command. To disable this feature, use the **ipv6 dhcp-relay bulk-lease**command with the **disable** keyword.

Examples

The following example shows how to set the bulk lease query data transfer timeout to 60 seconds:

```
Router(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```

Related Commands

Command	Description

ipv6 dhcp-relay show bindings

To enable the DHCPv6 relay agent to list prefix delegation (PD) bindings, use the **ipv6 dhcp-relay show bindings**command in global configuration mode. To disable PD binding tracking, use the no form of this command.

ipv6 dhcp-relay show bindings
no ipv6 dhcp-relay show bindings

Syntax Description   This command has no arguments or keywords.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines   The **ipv6 dhcp-relay show bindings** command lists the PD bindings that the relay agent is tracking. The command lists the bindings in the relay's radix tree, lists DHCPv6 relay routes, and prints each entry's prefix and length, client identity association identification (IAID), and lifetime. <<Any more information here?>>

Examples   The following example enables the DHCPv6 relay agent to list PD bindings: <<OK?>>:

```
Router# ipv6 dhcp-relay show bindings
```

ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the **ipv6 dhcp-relay source-interface**command in global configuration mode. To remove the interface from use as the source, use the no form of this command.

ipv6 dhcp-relay source-interface *interface-type interface-number*
no ipv6 dhcp-relay source-interface *interface-type interface-number*

Syntax Description

interface-type interface-number	(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.

Command Default

The address of the server-facing interface is used as the IPv6 relay source.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the **ipv6 dhcp relay source-interface** command in interface configuration mode) takes precedence over the global configuration if both have been configured.

Examples

The following example configures the Loopback 0 interface to be used as the relay source:

```
Router(config)# ipv6 dhcp-relay source-interface loopback 0
```

Related Commands

Command	Description
ipv6 dhcp relay source-interface	Enables DHCP for IPv6 service on an interface.

ipv6 dhcp server

To enable Dynamic Host Configuration Protocol (DHCP) for IPv6 service on an interface, use the **ipv6 dhcp server** in interface configuration mode. To disable DHCP for IPv6 service on an interface, use the **no** form of this command.

ipv6 dhcp server [{*poolname* | **automatic**}] [**rapid-commit**] [**preference** *value*] [**allow-hint**]
no ipv6 dhcp server

Syntax Description

poolname	(Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
automatic	(Optional) Enables the server to automatically determine which pool to use when allocating addresses for a client.
rapid-commit	(Optional) Allows the two-message exchange method for prefix delegation.
preference *value*	(Optional) Specifies the preference value carried in the preference option in the advertise message sent by the server. The range is from 0 to 255. The preference value defaults to 0.
allow-hint	(Optional) Specifies whether the server should consider delegating client suggested prefixes. By default, the server ignores client-hinted prefixes.

Command Default

DHCP for IPv6 service on an interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(24)T	The **automatic** keyword was added.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 dhcp server** command enables DHCP for IPv6 service on a specified interface using the pool for prefix delegation and other configuration through that interface.

The **automatic** keyword enables the system to automatically determine which pool to use when allocating addresses for a client. When an IPv6 DHCP packet is received by the server, the server determines if it was received from a DHCP relay or if it was directly received from the client. If the packet was received from a

relay, the server verifies the link-address field inside the packet associated with the first relay that is closest to the client. The server matches this link address against all address prefix and link-address configurations in IPv6 DHCP pools to find the longest prefix match. The server selects the pool associated with the longest match.

If the packet was directly received from the client, the server performs this same matching, but it uses all the IPv6 addresses configured on the incoming interface when performing the match. Once again, the server selects the longest prefix match.

The **rapid-commit** keyword enables the use of the two-message exchange for prefix delegation and other configuration. If a client has included a rapid commit option in the solicit message and the **rapid-commit** keyword is enabled for the server, the server responds to the solicit message with a reply message.

If the **preference** keyword is configured with a value other than 0, the server adds a preference option to carry the preference value for the advertise messages. This action affects the selection of a server by the client. Any advertise message that does not include a preference option is considered to have a preference value of 0. If the client receives an advertise message that includes a preference option with a preference value of 255, the client immediately sends a request message to the server from which the advertise message was received.

If the **allow-hint** keyword is specified, the server will delegate a valid client-suggested prefix in the solicit and request messages. The prefix is valid if it is in the associated local prefix pool and it is not assigned to a device. If the **allow-hint** keyword is not specified, a hint is ignored and a prefix is delegated from the free list in the pool.

The DHCP for IPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is already enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed:

```
Interface is in DHCP client mode
Interface is in DHCP server mode
Interface is in DHCP relay mode
```

Examples

The following example enables DHCP for IPv6 for the local prefix pool named server1:

```
Router(config-if)# ipv6 dhcp server server1
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
show ipv6 dhcp interface	Displays DHCP for IPv6 interface information.

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable**command in global configuration mode. To disable the feature, use the **no** form of this command.

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable

Syntax Description   This command has no arguments or keywords.

Command Default   The DHCPv6 server VRF-aware feature is not enabled on the router.

Command Modes

Global configuration (config)

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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines   The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on the router.

Examples   The following example enables the DHCPv6 server VRF-aware feature globally on the router:

```
Router(config)# ipv6 dhcp server option vpn
```

ipv6 eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 on a specified interface, use the **ipv6 eigrp** command in interface configuration mode. To disable EIGRP for IPv6, use the **no** form of this command.

ipv6 eigrp *as-number*
no ipv6 eigrp *as-number*

Syntax Description

as-number	Autonomous system number.

Command Default   EIGRP is not enabled on an IPv6 interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines   Use the **ipv6 eigrp** command to enable EIGRP for IPv6 on a per-interface basis.

If an autonomous system is specified, EIGRP for IPv6 is enabled only for the specified autonomous system. Otherwise, EIGRP for IPv6 is specified throughout the interface.

Examples   The following example enables EIGRP for IPv6 for AS 1 on Ethernet interface 0:

```
Router(config)# interface ethernet0
Router(config-if)# ipv6 eigrp 1
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 router eigrp	Configures the EIGRP routing process in IPv6.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable**command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6   enable
no   ipv6   enable

Syntax Description   This command has no arguments or keywords.

Command Default   IPv6 is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines   The **ipv6 enable**command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing. The no **ipv6 enable**command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples   The following example enables IPv6 processing on Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.
ipv6 address eui-64	Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.
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.

ipv6 general-prefix

To define an IPv6 general prefix, use the **ipv6 general-prefix** command in global configuration mode. To remove the IPv6 general prefix, use the **no** form of this command.

ipv6 general-prefix *prefix-name* {*ipv6-prefix/prefix-length* | **6to4** *interface-type interface-number* | **6rd** *interface-type interface-number*}
no ipv6 general-prefix *prefix-name*

Syntax Description

prefix-name	The name assigned to the prefix.
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.
	When defining a general prefix manually, specify both the *ipv6-prefix* and **/** *prefix-length* arguments.
/ *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.
	When defining a general prefix manually, specify both the *ipv6-prefix* and **/** *prefix-length* arguments.
6to4	Allows configuration of a general prefix based on an interface used for 6to4 tunneling.
	When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number*argument.
interface-type interface-number	Interface type and number. For more information, use the question mark (**?**) online help function.
	When defining a general prefix based on a 6to4 interface, specify the **6to4** keyword and the *interface-type interface-number*argument.
6rd	Allows configuration of a general prefix computed from an interface used for IPv6 rapid deployment (6RD) tunneling.

Command Default   No general prefix is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	The optional **6rd** keyword was added.

Usage Guidelines	Use the ipv6 general-prefix command to define an IPv6 general prefix.
	A general prefix holds a short prefix, based on which a number of longer, more specific, prefixes can be defined. When the general prefix is changed, all of the more specific prefixes based on it will change, too. This function greatly simplifies network renumbering and allows for automated prefix definition.
	More specific prefixes, based on a general prefix, can be used when configuring IPv6 on an interface.
	When defining a general prefix based on an interface used for 6to4 tunneling, the general prefix will be of the form 2002:a.b.c.d::/48, where "a.b.c.d" is the IPv4 address of the interface referenced.
Examples	The following example manually defines an IPv6 general prefix named my-prefix:

```
Router(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

The following example defines an IPv6 general prefix named my-prefix based on a 6to4 interface:

```
Router(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

Related Commands

Command	Description
show ipv6 general-prefix	Displays information on general prefixes for an IPv6 addresses.