IPv6 Commands: d to im

data-glean

To enable IPv6 first-hop security binding table recovery using source (or 'data') address gleaning, or to generate syslog messages about unrecognized binding table entries following a recovery, use the **destination-glean** command in IPv6 snooping configuration mode. To disable binding table recovery, use the **no** form of this command.

data-glean {**recovery** | **log-only**} [{**dhcp** | **ndp**}]
no data-glean

Syntax Description

recovery	Enables binding table recovery using destination address gleaning.
log-only	Generates a syslog message about unrecognized binding table entries following a recovery.
dhcp	Specifies that destination addresses should be recovered from Dynamic Host Configuration Protocol (DHCP).
ndp	Specifies that destination addresses should be recovered from Neighbor Discovery Protocol (NDP).

Command Default

IPv6 first-hop security binding table recovery using destination address gleaning is not enabled.

Command Modes

IPv6 snooping configuration mode (config-ipv6-snooping)

Command History

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

Usage Guidelines

When you configure IPv6 source guard using the **ipv6 source-guard policy** command, you can then also configure IPv6 first-hop security binding table recovery.

The **ipv6 snooping policy** command allows you to configure a snooping policy. You can configure first-hop security binding table recovery as part of this policy. The snooping policy can then be attached to a port, VLAN, or interface (depending on the device being used) using the **ipv6 snooping attach-policy** command.

If you use the **data-glean** command with the **log-only** keyword, only a syslog message will be generated and no recovery will be attempted.

Examples

The following example shows that destination addresses should be recovered from DHCP:

```
Device(config-ipv6-snooping)# data-glean recovery dhcp
```

The following example shows that a syslog message will be generated for all missed destination addresses following a binding table recovery:

```
Device(config-ipv6-snooping)# data-glean log-only
```

Related Commands

Command	Description
ipv6 source-guard policy	Configures an IPv6 source guard policy.
ipv6 snooping policy	Enters IPv6 snooping configuration mode.

default (IPv6 OSPF)

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

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

Usage Guidelines

The command is removed if it is disabled by default.

Examples

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

```
default timers spf
```

default (OSPFv3)

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

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

Syntax Description

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

summary-prefix	(Optional) OSPFv3 summary prefix.

Command Default

This command is disabled by default.

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

Router(config-router-af)# default area 1
```

Related Commands

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

default-information originate (IPv6 IS-IS)

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

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

Syntax Description

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

Command Default

This feature is disabled.

Command Modes

Address family configuration

Command History

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

Usage Guidelines

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

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

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

A route map can be used for two purposes:

- Make the router generate default in its Level 1 LSPs.
- Advertise ::/0 conditionally.

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

Examples

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

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

Related Commands

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

default-information originate (IPv6 OSPF)

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

When you use this command for the OSPF for IPv6 process, the default network must reside in the routing table, and you must satisfy the **route-map** *map-name* keyword and argument. Use the **default-information originate always route-map** *map-name* form of the command when you do not want the dependency on the default network in the routing table.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPF for IPv6 routing domain, an external metric type of type 2, and the default route to be always advertised:

```
default-information originate always metric 100 metric-type 2
```

Related Commands

Command	Description
redistribute (IPv6)	Redistributes IPv6 routes from one routing domain into another routing domain.

default-information originate (OSPFv3)

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

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

Command History

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

Usage Guidelines

Whenever you use the **redistribute** or the **default-information** command to redistribute routes into an OSPFv3 routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a *default route* into the OSPF for IPv6 routing

domain. The software still must have a default route for itself before it generates one, except when you have specified the **always** keyword.

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

Examples

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

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

default-metric (OSPFv3)

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

default-metric *metric-value*
no default-metric *metric-value*

Syntax Description

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

Command Default

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

Command Modes

OSPFv3 router configuration mode (config-router)

IPv6 address family configuration (config-router-af)

IPv4 address family configuration (config-router-af)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

You can gain finer control over the metrics of redistributed routes by using the options for the **redistribute** command.

Examples

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

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

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

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

Related Commands

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

deny (IPv6)

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

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

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

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

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

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, **udp**, or **hbh**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.
source-ipv6-prefix/prefix-length	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.

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

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

routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Allows routing headers with a value in the type field to be matched independently. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header
sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
undetermined-transport	(Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the “Usage Guidelines” section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration (config-ipv6-acl)#

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Aggregation Series Routers.
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.2(3)T	This command was modified. Support was added for the **hbh** keyword.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header

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

Examples

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

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

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

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

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

Related Commands

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

deny global-autoconf

To deny data traffic from autoconfigured global addresses, use the **deny global-autoconf** command in source-guard policy configuration mode or switch integrated security features source-guard policy configuration mode. To disable this function, use the **no** form of this command.

deny global-autoconf
no deny global-autoconf

Syntax Description

This command has no arguments or keywords.

Command Default

Data traffic is not denied.

Command Modes

Source-guard policy configuration mode (config-source-guard)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

Use the **deny global-autoconf** command to deny data traffic from auto-configured global addresses. This function is useful when all global addresses on a link are assigned by DHCP and the administrator wants to block hosts with self-configured addresses to send traffic. Use of this command also reduces the number of ternary content addressable memory (TCAM) entries that are used.

Examples

```
Device(config)# ipv6 source-guard policy
Device(config-source-guard)# deny global-autoconf
```

Related Commands

Command	Description
ipv6 source-guard policy	Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.

destination-glean

To enable IPv6 first-hop security binding table recovery using destination address gleaning, or to generate syslog messages about unrecognized binding table entries following a recovery, use the **destination-glean** command in IPv6 snooping configuration mode. To disable binding table recovery, use the **no** form of this command.

destination-glean {**recovery** | **log-only**} [{**dhcp**}]
no destination-glean

Syntax Description

recovery	Enables binding table recovery using destination address gleaning.
log-only	Generates a syslog message about unrecognized binding table entries following a recovery.
dhcp	Specifies that destination addresses should be recovered from Dynamic Host Configuration Protocol (DHCP).

Command Default

IPv6 first-hop security binding table recovery using destination address gleaning is not enabled.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

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

When you configure IPv6 destination guard using the **ipv6 destination-guard policy** command, you can then also configure IPv6 first-hop security binding table recovery.

The **ipv6 snooping policy** command allows you to configure a snooping policy. You can configure first-hop security binding table recovery as part of this policy. The snooping policy can then be attached to a port, VLAN, or interface (depending on the device being used) using the **ipv6 snooping attach-policy** command.

If you use the **destination-glean** command with the **log-only** keyword, only a syslog message will be generated and no recovery will be attempted.

Examples

The following example shows that destination addresses should be recovered from DHCP:

```
Device(config-ipv6-snooping)# destination-glean recovery dhcp
```

The following example shows that a syslog message will be generated for all missed destination addresses following a binding table recovery:

```
Device(config-ipv6-snooping)# destination-glean log-only
```

Related Commands

Command	Description
ipv6 destination-guard policy	Configures an IPv6 destination guard policy.
ipv6 snooping policy	Enters IPv6 snooping configuration mode.

device-role

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode or router advertisement (RA) guard policy configuration mode.

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

Syntax Description

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

Command Default

The device role is host.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE. The **monitor** and **router** keywords were deprecated only from the ND inspection policy configuration (config-nd-inspection) command mode; they continue to be available in the RA guard policy configuration (config-ra-guard) mode.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The **monitor** and **router** keywords were deprecated only from the ND inspection policy configuration (config-nd-inspection) command mode; they continue to be available in the RA guard policy configuration (config-ra-guard) mode.

Usage Guidelines

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

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

Note With the introduction of Cisco IOS Release 15.2(4)S1, the trusted port has precedence over the device role for accepting RAs over a port to the router. Prior to this release, the device role router had precedence over the trusted port. The device role of the router still needs to be configured in order for the RS to be sent over the port.

Examples

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

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

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

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

Related Commands

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

discard-route (IPv6)

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

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

Syntax Description

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

Command Default

External and internal discard route entries are installed.

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
Router# show ipv6 route
IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/32 [110/0]
     via ::, Null0
C   2001:0:11::/64 [0/0]
     via ::, Ethernet0/0
L   2001:0:11:0:A8BB:CCFF:FE00:6600/128 [0/0]
```

```
     via ::, Ethernet0/0
C    2001:1:1::/64 [0/0]
     via ::, Ethernet1/0
L    2001:1:1:0:A8BB:CCFF:FE00:6601/128 [0/0]
     via ::, Ethernet1/0
L    FE80::/10 [0/0]
     via ::, Null0
L    FF00::/8 [0/0]
     via ::, Null0
Router# show ipv6 route ospf
IPv6 Routing Table - 7 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O    2001::/32 [110/0]
     via ::, Null0
```

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

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipv6 router ospf 1
Router(config-router)# no discard-route internal
Router(config-router)# end
Router# show ipv6 route ospf
IPv6 Routing Table - 6 entries
Codes:C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

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

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

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

```
Router# show running-config
Building configuration...
Current configuration :2490 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
```

```
logging snmp-authfail
logging buffered 20480 debugging
logging console warnings
!
clock timezone PST -8
clock summer-time PDT recurring
no aaa new-model
ip subnet-zero
no ip domain lookup
!
!
ip audit po max-events 100
ipv6 unicast-routing
no ftp-server write-enable
!
.
.
.
interface Ethernet0/0
 no ip address
 ipv6 address 2001:0:11::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 0
 no cdp enable
!
interface Ethernet1/0
 no ip address
 ipv6 address 2001:1:1::/64 eui-64
 ipv6 enable
 ipv6 ospf 1 area 1
 no cdp enable
 .
 .
 .
ipv6 router ospf 1
 router-id 2.0.0.1
 log-adjacency-changes
 no discard-route external
 no discard-route internal
 area 0 range 2001::/32
 redistribute rip 1
!
```

Related Commands

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

distance (IPv6)

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

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

Syntax Description

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

Command Default

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

Command Modes

Address family configuration
Router configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

distance (IPv6 EIGRP)

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

distance *internal-distance external-distance*
no distance

Syntax Description

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

Command Default

internal-distance : 90*external-distance*: 170

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

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

The table below lists the default administrative distances.

Table 1: Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5

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

Examples

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

```
distance 95 165
```

distance (IPv6 Mobile)

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

distance [*mobile-distance*]
no distance

Syntax Description

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

Command Default

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

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

distance (OSPFv3)

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

distance *distance*
no distance *distance*

Syntax Description

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

Command Default

Administrative distance is 110.

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

distance bgp (IPv6)

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

distance bgp *external-distance internal-distance local-distance*
no distance bgp

Syntax Description

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

Command Default

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

Command Modes

Address family configuration

Command History

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

Usage Guidelines

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

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1

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

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

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

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

Examples

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

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

Related Commands

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

distribute-list prefix-list (IPv6 EIGRP)

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

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

Syntax Description

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

Command Default

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

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

distribute-list prefix-list (IPv6 OSPF)

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

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

Syntax Description

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

Command Default

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

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

distribute-list prefix-list (IPv6 RIP)

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

distribute-list prefix-list *listname* {**in** | **out**} [*interface-type interface-number*]
no distribute-list prefix-list *listname*

Syntax Description

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

Command Default

Prefix lists are not applied to IPv6 RIP routing updates.

Command Modes

Router configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

distribute-list prefix-list (OSPFv3)

To apply a prefix list to Open Shortest Path First version 3 (OSPFv3) routing updates that are received or sent on an interface, use the **distribute-list prefix-list** command in IPv6 or IPv4 address family configuration mode. To remove the prefix list, use the **no** form of this command.

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

Syntax Description

list-name	Name of a prefix list. The list defines which OSPFv3 networks are to be accepted in incoming routing updates and which networks are to be advertised in outgoing routing updates, based upon matching the network prefix to the prefixes in the list.
in	Applies the prefix list to incoming routing updates on the specified interface.
interface-type interface-number	(Optional) Interface type and number. For more information, use the question mark (**?**) online help function.
out	Restricts which prefixes OSPFv3 will identify to the other protocol.
routing-process	Name of a specific routing process. Valid entries for this value are **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip,** or **static**.
as-number	(Optional) Autonomous system number, required for use with Border Gateway Protocol (BGP) and Routing Information Protocol (RIP).

Command Default

Prefix lists are not applied to OSPFv3 routing updates.

Command Modes

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

Command History

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

Usage Guidelines

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

Examples

The following example enters IPv6 address family configuration mode, applies prefix list PL1 to routes received on Ethernet interface 0/0, and applies prefix list PL2 to advertised routes that came from process bgp 65:

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

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

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode for OSPFv3.
address-family ipv6	Enters IPv6 address family configuration mode for OSPFv3.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or prefix list entries.

dns-server (IPv6)

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

dns-server *ipv6-address*
no dns-server *ipv6-address*

Syntax Description

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

Command Default

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

Command Modes

DHCP for IPv6 pool configuration

Command History

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

Usage Guidelines

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

Examples

The following example specifies the DNS IPv6 servers available:

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

Related Commands

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

domain-name (IPv6)

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

domain-name *domain-name*
no domain-name

Syntax Description

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

Command Default

No default domain name is defined for the DNS view.

Command Modes

DHCPv6 pool configuration mode (config-dhcp)

Command History

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

Usage Guidelines

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

Examples

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

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

drop-unsecure

To drop messages with no or invalid options or an invalid signature, use the **drop-unsecure**command in neighbor discovery (ND) inspection policy configuration mode or or router advertisement (RA) guard policy configuration mode. To disable this function, use the **no** form of this command.

drop-unsecure
no drop-unsecure

Syntax Description

This command has no arguments or keywords.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

enforcement

To set the enforcement level of a destination guard policy, use the **enforcement** command in destination-guard configuration mode.

enforcement {**always** | **stressed**}

Syntax Description

always	Sets the enforcement level to always.
stressed	Sets the enforcement level to forced only when the system is under stress.

Command Default

The enforcement level of a destination guard policy is set to always.

Command Modes

Destination-guard configuration (config-destguard)

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

Depending on the network architecture, the sources of binding table information, and the degree of change in the system, the binding table may not always have complete information about the node membership of a VLAN. The enforcement level policy element means that systems with authoritative knowledge of the VLAN membership should set the enforcement level to always. Systems with less confidence, or those with a strong desire to avoid inadvertent packet loss, should set the enforcement level to stressed.

Examples

The following example shows how to set the enforcement level to always:

```
Device(config)# ipv6 destination-guard policy destination
Device(config-destguard)# enforcement always
```

Related Commands

Command	Description
ipv6 destination-guard policy	Defines the destination guard policy.

eui-interface

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

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

Syntax Description

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

Command Default

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

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

evaluate (IPv6)

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

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

Syntax Description

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

Command Default

IPv6 reflexive access lists are not evaluated.

Command Modes

IPv6 access list configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

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

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

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

Related Commands

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

event-log (OSPFv3)

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

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

Syntax Description

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

Command Default

Event logging is not enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

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

Usage Guidelines

<<Need some guidelines>>

Examples

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

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

Related Commands

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

explicit-prefix

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

explicit-prefix
no explicit-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No IPv6 prefixes are specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

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

Examples

The following example shows how to register connected IPv6 prefixes:

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

Related Commands

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

frame-relay map ipv6

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

frame-relay map ipv6 *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
no frame-relay map ipv6 *ipv6-address*

Syntax Description

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

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

Command Default

No mapping is defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

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

Note Given that each PVC in the following example is configured on a different point-to-point subinterface, the configuration in the following example can also be used in a network that is not fully meshed. Additionally, configuring each PVC on a different point-to-point subinterface can help simplify your routing protocol configuration. However, the configuration in the following example requires more than one IPv6 network, whereas configuring each PVC on point-to-multipoint interfaces requires only one IPv6 network.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
!
interface Serial3.17 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1017::46/64
 frame-relay interface-dlci 17
!
interface Serial3.19 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1019::46/64
 frame-relay interface-dlci 19
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
!
interface Serial5.17 point-to-point
 description to Cisco A
```

```
 ipv6 address 2001:0DB8:2222:1017::73/64
 frame-relay interface-dlci 17
!
interface Serial5.18 point-to-point
 description to Cisco C
 ipv6 address 2001:0DB8:2222:1018::73/64
 frame-relay interface-dlci 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
!
interface Serial0.18 point-to-point
 description to Cisco B
 ipv6 address 2001:0DB8:2222:1018::72/64
 frame-relay interface-dlci 18
!
interface Serial0.19 point-to-point
 description to Cisco A
 ipv6 address 2001:0DB8:2222:1019::72/64
 frame-relay interface-dlci 19
```

In the following example, the same three nodes (Cisco A, Cisco B, and Cisco C) from the previous example make up a fully meshed network and each node is configured with two PVCs (which provide an individual connection to each of the other two nodes). However, the two PVCs on each node in the following example are configured on a single interface (serial 3, serial 5, and serial 10, respectively), which makes each interface a point-to-multipoint interface. Therefore, explicit mappings are required between the link-local and global IPv6 addresses of each interface on all three nodes and the DLCI (DLCI 17, 18, and 19) of the PVC used to reach the addresses.

Cisco A Configuration

```
interface Serial3
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::46/64
 frame-relay map ipv6 FE80::E0:F727:E400:A 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 19 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::72 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 17
```

Cisco B Configuration

```
interface Serial5
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::73/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 17 broadcast
 frame-relay map ipv6 FE80::60:3E47:AC8:8 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 17
 frame-relay map ipv6 2001:0DB8:2222:1044::72 18
```

Cisco C Configuration

```
interface Serial0
 encapsulation frame-relay
 ipv6 address 2001:0DB8:2222:1044::72/64
 frame-relay map ipv6 FE80::60:3E59:DA78:C 19 broadcast
 frame-relay map ipv6 FE80::E0:F727:E400:A 18 broadcast
 frame-relay map ipv6 2001:0DB8:2222:1044::46 19
 frame-relay map ipv6 2001:0DB8:2222:1044::73 18
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay payload-compress	Enables Stacker payload compression on a specified point-to-point interface or subinterface.

glbp ipv6

To activate the Gateway Load Balancing Protocol (GLBP) in IPv6, use the **glbp ipv6**command in interface configuration mode. To disable GLBP, use the **no**form of this command.

glbp *group* **ipv6** [{*ipv6-address* | **autoconfig**}]
no glbp *group* **ipv6** [{*ipv6-address* | **autoconfig**}]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
ip-address	(Optional) Virtual IPv6 address for the GLBP group. The IPv6 address must be in the same subnet as the interface IPv6 address.
autoconfig	(Optional) Indicates a default IPv6 address can be created based on a MAC address.

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **glbp ipv6** command activates GLBP on the configured interface. If an IPv6 address is specified, that address is used as the designated virtual IPv6 address for the GLBP group. If no IPv6 address is specified, the designated address is learned from another router configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one router on the cable must have been configured with the designated address. A router must be configured with, or have learned, the virtual IPv6 address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ipv6** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IPv6 address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Examples

The following example enables GLBP on an IPv6 configured interface:

```
Router(config-if)# glbp ipv6
```

Related Commands

Command	Description
glbp ip	Activates the GLBP in IPv4.

Command	Description
show glbp	Displays GLBP information.

graceful-restart

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-capable router, use the **graceful-restart**command in OSPF router configuration mode. To disable graceful restart, use the **no** form of this command.

graceful-restart [**restart-interval** *interval*]
no graceful-restart

Syntax Description

restart-interval *interval*	(Optional) Graceful-restart interval in seconds. The range is from 1 to 1800, and the default is 120.

Command Default

The GR feature is not enabled on GR-capable routers.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
15.1(1)SY	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **graceful-restart** command can be enabled only on GR-capable routers.

Examples

The following examples enables graceful restart mode on a GR-capable router in IPv6 and IPv4:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restar
```

The following examples enables graceful restart mode on a GR-capable router in IPv6 only:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart
```

Related Commands

Command	Description
graceful-restart helper	Enables the OSPFv3 graceful restart feature on a GR-aware router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

graceful-restart helper

To enable the Open Shortest Path First version 3 (OSPFv3) graceful restart feature on a graceful-restart-aware router, use the **graceful-restart helper**command in OSPFv3 router configuration mode. To reset the router to its default, use the **no** form of this command.

graceful-restart helper {**disable** | **strict-lsa-checking**}
no graceful-restart helper

Syntax Description

disable	Disables graceful-restart-aware mode.
strict-lsa-checking	Enables graceful restart-helper mode with strict link-state advertisement (LSA) checking.

Command Default

Graceful restart-aware mode is enabled.

Command Modes

OSPFv3 router configuration mode (config-router)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(3)S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
Cisco IOS XE Release 3.4S	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
15.2(1)T	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.
15.1(1)SY	This command was modified. The feature can be enabled in an IPv4 or IPv6 OSPFv3 process. The **disable** and **strict-lsa-checking** keywords can be used only in an IPv6 OSPFv3 process.

Usage Guidelines

GR-helper mode is configurable on both GR-aware and GR-capable routers; however, GR-aware routers can use only the **graceful-restart helper** command.

The **strict-lsa-checking** keyword indicates whether an OSPFv3 GR-aware router should terminate the helper function when there is a change to an LSA that would be flooded to the restarting router or when there is a changed LSA on the restarting router's retransmission list when graceful restart is initiated.

Examples

The following example enables GR-helper mode with strict LSA checking:

```
Router(config)# ipv6 router ospf 1234
Router(config-router)# graceful-restart helper strict-lsa-checking
```

The following example shows how to enable GR-helper mode in an OSPFv3 IPv4 instance:

```
Router(config)# ospfv3 router 1
Router(config-router)# graceful-restart helper
```

Related Commands

Command	Description
graceful-restart	Enables the OSPFv3 GR feature on a graceful-restart-capable router.
router ospfv3	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

hardware statistics

To enable the collection of hardware statistics, use the **hardware statistics**command in IPv6or IPv4 access-list configuration mode. To disable this feature, use the **no** form of this command.

hardware statistics
no hardware statistics

Syntax Description

This commands has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

IPv6 access-list configuration (config-ipv6-acl)

Command History

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

Usage Guidelines

The hardware statistics command affects only global access-list (ACL) counters.

Examples

The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```

home-address

To specify the mobile router home address using an IPv6 address or interface identifier, use the **home-address**command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-address {**home-network***ipv6-address-identifier* | **interface**}
no home-address

Syntax Description

home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6-address-identifier	The IPv6 home address identifier.
interface	Specifies the interface to use to identify the home address.

Command Default

No IPv6 home address is specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

The **home-address**command allows you to specify the IPv6 home address. When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-network	Specifies the home network's IPv6 prefix on the mobile router.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

home-network

To specify the home network's IPv6 prefix on the mobile router, use the **home-network**command in IPv6 mobile router configuration mode. To disable this function, use the **no** form of this command.

home-network *ipv6-prefix*
no home-network

Syntax Description

ipv6-prefix	The IPv6 prefix of the home network.

Command Default

The IPv6 home network prefix is not specified.

Command Modes

IPv6 mobile router configuration (IPv6-mobile-router)

Command History

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

Usage Guidelines

Users can configure up to 10 home-network entries, and they are used in order of priority. The prefix identifies the home network of the mobile router and is used to discover when the mobile router is at home.

When multiple home networks have been configured, we recommend that you use the **home-address home-network** command syntax, so that the mobile router builds a home address that matches the home network to which it registers.

The command syntax sorts the home networks by priority. The default priority is 128. The home networks will be tried from the smaller to the higher value and, for a same priority, the addresses without the discover keyword are tried first.

Examples

The following example shows multiple configured home networks and enables the mobile router to build a home address that matches its registered home network:

```
Router(config)# ipv6 mobile router
Router(IPv6-mobile-router)# eui-interface Ethernet0/0
Router(IPv6-mobile-router)# home-network 2001:0DB8:1/64 priority 18
Router(IPv6-mobile-router)# home-network 2001:0DB8:2/64
Router(IPv6-mobile-router)# home-network 2001:0DB8:3/64 discover
Router(IPv6-mobile-router)# home-network 2001:0DB8:4/64 priority 200
Router(IPv6-mobile-router)# home-address home-network eui-64
```

Related Commands

Command	Description
home-address	Specifies the mobile router home address using an IPv6 address or interface identifier.
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in RA guard policy configuration mode.

hop-limit {**maximum** | **minimum** } *limit*

Syntax Description

maximum *limit*	Verifies that the hop-count limit is lower than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

Related Commands

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

host group

To create a host group configuration in IPv6 Mobile, use the **host group**command in home agent configuration mode. To remove a host configuration, use the **no** form of this command.

host group *profile-name*
no host group *profile-name*

Syntax Description

profile-name	Specifies a name for the host group.

Command Default

No IPv6 Mobile host configurations exist.

Command Modes

Home agent configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **host group** command creates an IPv6 Mobile home-agent host configuration with a given profile name. Multiple instances with different profile names can be created and used.

Do not configure two separate groups with the same IPv6 address. For example, host group group1 and host group group2 cannot both be configured with the same IPv6 address of baba::1.

Examples

In the following example, the user enters home agent configuration mode and creates a host group named group1:

```
Router(config)# ipv6 mobile home-agent
Router(config-ha)# host group group1
```

Related Commands

Command	Description
address (IPv6 mobile router)	Specifies the home address of the IPv6 Mobile node.
ipv6 mobile home-agent (global configuration)	Enters home agent configuration mode.
nai	Specifies the NAI for the IPv6 mobile node.

identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the **identity**command in IKEv2 keyring peer configuration mode. To remove the identity, use the **no** form of this command.

identity {**address**{*ipv4-addressipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *domain-name*}
no identity {**address**{*ipv4-addressipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address to identify the peer.
fqdn domain *domain-name*	Uses the Fully Qualified Domain Name (FQDN) to identify the peer.
email domain*domain-name*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietary types to identify the peer.

Command Default

Identity types are not specified to a peer.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.3(3)M	This command was modified. The **domain** *domain-name* keyword-argument pair was added.

Usage Guidelines

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an e-mail ID, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session, and the initiator looks up keys during session startup.

Examples

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 or IPv6 address or the range of the peers in an IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

identity local

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the **identity local**command in IKEv2 profile configuration mode. To remove the identity, use the **no** form of this command.

identity local {**address**{*ipv4-addressipv6-address*} | **dn** | **fqdn** *fqdn-string* | **email** *e-mail-string* | **key-id** *opaque-string*}
no identity

Syntax Description

address *{ipv4-address | ipv6-address}*	Uses the IPv4 or IPv6 address as the local identity.
dn	Uses the distinguished name as the local identity.
fqdn *fqdn-string*	Uses the Fully Qualified Domain Name (FQDN) as the local identity.
email *email-string*	Uses the e-mail ID as the local identity.
key-id *opaque-string*	Uses the proprietary type opaque string as the local identity.

Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6). If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.

Note You can configure one local IKEv2 identity type for a profile.

Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
```

```
Router(config-ikev2-profile)# identity local address 10.0.0.1
The following example shows how to specify an IPv6 address as the local IKEv2 identity:
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

import dns-server

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

import dns-server
no import dns-server

Syntax Description

This command has no arguments or keywords.

Command Default

The DNS recursive name server list is not imported to a client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The DNS recursive name server option provides a list of one or more IPv6 addresses of DNS recursive name servers to which a client's DNS resolver may send DNS queries. The DNS servers are listed in the order of preference for use by the client resolver.

The DNS recursive name server list option code is 23. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a list of available DNS recursive name servers to a client:

```
Router(config-dhcp)# import dns-server
```

Related Commands

Command	Description
import domain-name	Imports the domain search list option to a DHCP for IPv6 client.

import domain-name

To import the domain name search list option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name search list, use the **no** form of this command.

import domain-name
no import domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

The domain search list is not imported to the client.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The domain name search list option specifies the domain search list the client is to use when resolving hostnames with DNS.

The domain name search list option code is 24. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import a domain search list to the client:

```
Router(config-dhcp)# import domain-name
```

Related Commands

Command	Description
import dns-server	Imports the DNS recursive name server option to a DHCP for IPv6 client.

import information refresh

To import the information refresh time option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

import information refresh
no import information refresh

Syntax Description

This command has no arguments or keywords.

Command Default

The information refresh time option is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCP for IPv6. It is used only in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the information refresh time:

```
import information refresh
```

Related Commands

Command	Description
information refresh	Specifies the information refresh time to be sent to the client.

import nis address

To import the network information service (NIS) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nis address
no import nis address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The NIS servers option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS servers option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS address of an IPv6 server:

```
import nis address
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nis domain-name

To import the network information service (NIS) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nis domain-name** command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nis domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS domain name is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The NIS domain name option provides a NIS domain name for the client.

The NIS domain name option code is 29.

Examples

The following example shows how to import a client's NIS domain name:

```
import nis domain-name
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

import nisp address

To import the network information service plus (NIS+) servers option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp address** command in IPv6 DHCP pool configuration mode. To remove the NIS address, use the **no** form of this command.

import nisp address
no import nisp address

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ address of an IPv6 server:

```
import nisp address
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import nisp domain-name

To import the network information service plus (NIS+) domain name option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import nisp domain-name**command in IPv6 DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

import nisp domain-name
no import nisp domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The NIS+ domain name option provides an NIS+ domain name for the client.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to import the NIS+ domain name of a client:

```
import nisp domain-name
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ server option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

import sip address

To import the Session Initiation Protocol (SIP) server IPv6 address list option to the outbound SIP proxy server, use the **import sip address**command in IPv6 DHCP pool configuration mode. To remove the SIP server IPv6 address list, use the **no** form of this command.

import sip address
no import sip address

Syntax Description

This command has no arguments or keywords.

Command Default

SIP IPv6 address list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server IPv6 address list option specifies a list of IPv6 addresses that indicate SIP outbound proxy servers available to the client. Servers must be listed in order of preference.

The SIP server IPv6 address list option code is 22. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server IPv6 address list to the client:

```
Router(config-dhcp)# import
 sip address
```

Related Commands

Command	Description
import sip domain-name	Imports a SIP server domain-name list option to the outbound SIP proxy server.

import sip domain-name

To import a Session Initiation Protocol (SIP) server domain-name list option to the outbound SIP proxy server, use the **import sip domain-name**command in IPv6 DHCP pool configuration mode. To remove the SIP server domain-name list, use the **no** form of this command.

import sip domain-name
no import sip domain-name

Syntax Description

This command has no arguments or keywords.

Command Default

SIP domain-name list is not imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

A SIP server is the host on which the outbound SIP proxy server is running.

The SIP server domain-name list option contains the domain names of the SIP outbound proxy servers. Domain names must be listed in order of preference. The option may contain multiple domain names, but the client must try the records in the order listed. The client resolves the subsequent domain names only if attempts to contact the first one failed or yielded no common transport protocols between client and server or denoted a domain administratively prohibited by client policy.

The SIP server domain-name list option code is 21. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example enables the user to import a SIP server domain-name list to the client:

```
Router(config-dhcp)# import sip domain-name
```

Related Commands

Command	Description
import sip address	Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

import sntp address

To import the Simple Network Time Protocol (SNTP) address option to a Dynamic Host Configuration Protocol (DHCP) for IPv6 client, use the **import sntp address** command in IPv6 DHCP pool configuration mode. To remove the SNTP server address, use the **no** form of the command.

import sntp address *ipv6-address*
no import sntp address *ipv6-address*

Syntax Description

ipv6-address	(Optional) The IPv6 address for SNTP. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

Command Default

No SNTP server address is imported.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

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

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

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

Examples

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

```
import sntp address
```

Related Commands

Command	Description
sntp address	Specifies the SNTP server to be sent to the client.

information refresh

To specify the information refresh time to be sent to the client, use the **information refresh**command in IPv6 DHCP pool configuration mode. To remove the specified refresh time, use the **no** form of this command.

information refresh {*days* [*hours minutes*] | **infinity**}
no information refresh {*days* [*hours minutes*] | **infinity**}

Syntax Description

days	Refresh time specified in number of days. The default is 0 0 86400, which equals 24 hours.
hours	(Optional) Refresh time specified in number of hours.
minutes	(Optional) Refresh time specified in number of minutes. The minimum refresh time that can be used is 0 0 600, which is 10 minutes.
infinity	Sets the IPv6 value of 0xffffffff used to configure the information refresh time to infinity.

Command Default

Information refresh information is not sent to the client. The client refreshes every 24 hours if no refresh information is sent.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

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

The information refresh time option specifies the maximum time a client should wait before refreshing information retrieved from DHCP for IPv6. It is only used in Reply messages in response to Information Request messages. In other messages, there will usually be other options that indicate when the client should contact the server (for example, addresses with lifetimes).

The maximum value for the information refresh period on the DHCP for IPv6 client is 7 days. The maximum value is not configurable.

The information refresh time option code is 32. For more information on DHCP options and suboptions, see the "DHCP Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the information refresh time to be 1 day, 1 hour, and 1 second:

```
information refresh 1 1 1
```

Related Commands

Command	Description
import information refresh	Imports the information refresh time option to a DHCP for IPv6 client.