

ipv – ir

- ipv4-prefix, on page 3
- ipv6 address, on page 5
- ipv6-address-pool, on page 10
- ipv6-address-pools, on page 12
- ipv6 dhcp client pd, on page 14
- ipv6 dhcp client pd hint, on page 17
- ipv6 dhcp pool, on page 20
- ipv6 dhcprelay enable, on page 23
- ipv6 dhcp relay link-address, on page 25
- ipv6 dhcprelay server, on page 27
- ipv6 dhcprelay timeout, on page 29
- ipv6 dhcp server, on page 30
- ipv6 eigrp, on page 33
- ipv6 hello-interval eigrp, on page 34
- ipv6 hold-time eigrp, on page 35
- ipv6 router eigrp, on page 37
- ipv6 split-horizon eigrp, on page 39
- ipv6 summary-address eigrp, on page 40
- ipv6 enable, on page 42
- ipv6 enforce-eui64, on page 44
- ipv6 icmp, on page 46
- ipv6 local pool, on page 49
- ipv6 nd dad attempts, on page 51
- ipv6 nd managed-config-flag, on page 53
- ipv6 nd ns-interval, on page 54
- ipv6 nd other-config-flag, on page 55
- ipv6 nd prefix, on page 56
- ipv6 nd ra dns-search-list, on page 58
- ipv6 nd ra dns server, on page 60
- ipv6 nd ra-interval, on page 62
- ipv6 nd ra-lifetime, on page 64
- ipv6 nd reachable-time, on page 66
- ipv6 nd suppress-ra, on page 68

- ipv6 neighbor, on page 69
- ipv6 ospf, on page 71
- ipv6 ospf area, on page 73
- ipv6 ospf cost, on page 74
- ipv6 ospf database-filter all out, on page 75
- ipv6 ospf dead-interval, on page 76
- ipv6 ospf encryption, on page 77
- ipv6 ospf flood-reduction, on page 79
- ipv6 ospf hello-interval, on page 81
- ipv6 ospf mtu-ignore, on page 82
- ipv6 ospf neighbor, on page 83
- ipv6 ospf network, on page 85
- ipv6 ospf priority, on page 86
- ipv6 ospf retransmit-interval, on page 87
- ipv6 ospf transmit-delay, on page 88
- ipv6-prefix, on page 89
- ipv6 prefix-list, on page 91
- ipv6 route, on page 93
- ipv6 router ospf, on page 95
- ipv6-split-tunnel-policy, on page 98
- ipv6-vpn-address-assign, on page 100
- ipv6-vpn-filter, on page 102
- ip verify reverse-path, on page 104
- ipv6 unnumbered, on page 106

ipv4-prefix

To configure the IPv4 prefix for the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **ipv4-prefix** command in MAP domain basic mapping rule configuration mode. Use the **no** form of this command to remove the prefix.

ipv4-prefix*ipv4_network_addressnetmask*
no ipv4-prefix *ipv4_network_address netmask*

Syntax Description

ipv4_network_address netmask	The IPv4 prefix that defines the IPv4 address pool for the customer edge (CE) device. Specify a network address and subnet mask, for example, 192.168.3.0 255.255.255.0. You cannot use the same IPv4 prefix in different MAP domains.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain basic mapping rule configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The IPv4 prefix defines the IPv4 address pool for the customer edge (CE) device. The CE device first translates its IPv4 address to an address (and port number) in the pool defined by the IPv4 prefix. MAP then translates this new address to an IPv6 address using the prefix in the default mapping rule.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
```

```
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

ipv6 address

To enable IPv6 and configure the IPv6 addresses on an interface (in routed mode) or for the bridge group or management interface address (transparent mode), use the **ipv6 address** command. To remove the IPv6 addresses, use the **no** form of this command.

ipv6 prefix { **autoconfig** [**autoconfig** [**default trust** { **dhcp** | **ignore** }] | **dhcp** [**defualt**] | *ipv6_address* | *prefix_name ipv6_address* | *prefix_length* | *ipv6_address* **link-local** [**standby** *ipv6_adress*] }
no ipv6 prefix { **autoconfig** [**autoconfig** [**default trust** { **dhcp** | **ignore** }] | **dhcp** [**defualt**] | *ipv6_address* | *prefix_name ipv6_address* | *prefix_length* | *ipv6_address* **link-local** [**standby** *ipv6_adress*] }

Syntax Description

autoconfig	Enables stateless autoconfiguration on the interface. Enabling stateless autoconfiguration on the interface configures IPv6 addresses based on prefixes received in router advertisement messages. A link-local address, based on the modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled. Not supported for transparent firewall mode. **Note** Although RFC 4862 specifies that hosts configured for stateless autoconfiguration do not send router advertisement messages, the ASA does send router advertisement messages in this case. See the **ipv6 nd suppress-ra** command to suppress messages.
cluster-pool *poolname*	(Optional) For ASA clustering, sets the cluster pool of addresses defined by the **ipv6 local pool** command. The main cluster IP address defined by the argument belongs to the current master unit only. Each cluster member receives a local IP address from this pool. You cannot determine the exact address assigned to each unit in advance; to see the address used on each unit, enter the **show ipv6 local pool** *poolname* command. Each cluster member is assigned a member ID when it joins the cluster. The ID determines the local IP used from the pool.
default	(Optional) Obtains a default route from Router Advertisements.
default trust	(Optional) Installs a default route from Router Advertisements.
dhcp (autoconfig)	(Optional) Specifies the ASA only uses a default route from Router Advertisements that come from a trusted source (in other words, from the same server that provided the IPv6 address).
dhcp	Obtains the IPv6 address from a DHCPv6 server.
ignore	(Optional) Specifies that Router Advertisements can be sourced from another network, which can be a riskier method.
ipv6_address/prefix_length	Assigns a global address to the interface. When you assign a global address, the link-local address is automatically created for the interface.

ipv6_prefix/prefix_length **eui-64**	Assigns a global address to the interface by combining the specified prefix with an interface ID generated from the interface MAC address using the modified EUI-64 format. When you assign a global address, the link-local address is automatically created for the interface. If the value specified for the >*prefix_length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID. An error message will be displayed if another host is using the specified address. You do not need to specify the standby address; the interface ID will be generated automatically. The modified EUI-64 format interface ID is derived from the 48-bit link-layer (MAC) address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower three bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.
ipv6_address **link-local**	Manually configures the link-local address only. The *ipv6_address* specified with this command overrides the link-local address that is automatically generated for the interface. The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in modified EUI-64 format. An interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error message will be displayed if another host is using the specified address.
prefix_name ipv6_address/prefix_length	Uses a delegated prefix. This feature requires an ASA interface to have the DHCPv6 Prefix Delegation client enabled (**ipv6 dhcp client pd**). Typically, the delegated prefix will be /60 or smaller so you can subnet to multiple /64 networks. /64 is the supported subnet length if you want to support SLAAC for connected clients. You should specify an address that completes the /60 subnet, for example ::1:0:0:0:1. Enter :: before the address in case the prefix is smaller than /60. For example, if the delegated prefix is 2001:DB8:1234:5670::/60, then the global IP address assigned to this interface is 2001:DB8:1234:5671::1/64. The prefix that is advertised in router advertisements is 2001:DB8:1234:5671::/64. In this example, if the prefix is smaller than /60, the remaining bits of the prefix will be 0's as indicated by the leading ::. For example, if the prefix is 2001:DB8:1234::/48, then the IPv6 address will be 2001:DB8:1234::1:0:0:0:1/64.
standby *ipv6_address*	(Optional) Specifies the interface address used by the secondary unit or failover group in a failover pair.

Command Default

IPv6 is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.
8.2(2)	Support for a standby address was added.
8.4(1)	For transparent mode, bridge groups were added. You set the IP address for the BVI, and not globally.
9.0(1)	The **cluster-pool** keyword was added to support ASA clustering.
9.6(2)	We added the following options: • **autoconfig default trust** {**dhcp** | **ignore**} • **dhcp** [**default**] • *prefix_name ipv6_address/prefix_length*

Usage Guidelines

Configuring an IPv6 address on an interface enables IPv6 on that interface; you do not need to use the **ipv6 enable** command after specifying an IPv6 address.

Multiple Context Mode Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

DHCPv6 and prefix delegation options are not supported with multiple context mode.

Transparent Firewall Guidelines

Transparent mode only supports manually setting the IPv6 address. A transparent firewall does not participate in IP routing. The only IP configuration required for the ASA is to set the BVI address. This address is required because the ASA uses this address as the source address for traffic originating on the ASA, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context. For models that include a Management interface, you can also set an IP address for this interface for management purposes.

Failover Guidelines

The standby IP address must be on the same subnet as the main IP address.

ASA Clustering Guidelines

You can only set the cluster pool for an individual interface after you configure the cluster interface mode to be individual (**cluster-interface mode individual**). The only exception is for the management-only interface(s):

- You can always configure the management-only interface as an individual interface, even in spanned EtherChannel mode. The management interface can be an individual interface even in transparent firewall mode.
- In spanned EtherChannel mode, if you configure the management interface as an individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.

DHCPv6 and prefix delegation options are not supported with clustering.

Examples

The following example assigns 2001:0DB8:BA98::3210/64 as the global address for the selected interface and 2001:0DB8:BA98::3211 as the address for the corresponding interface on the standby unit:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

The following example assigns an IPv6 address automatically for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

The following example assigns IPv6 prefix 2001:0DB8:BA98::/64 to the selected interface and specifies an EUI-64 interface ID in the low order 64 bits of the address. If this device is part of a failover pair, you do not need to specify the **standby** keyword; the standby address will be automatically created using the modified EUI-64 interface ID.

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface on the primary unit in a failover pair, and FE80::260:3EFF:FE11:6671 as the link-level address for the corresponding interface on the secondary unit.

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

The following example assigns ::1:0:0:0:1/64 as the address to complete the Deligated Prefix:

```
ciscoasa(config)# interface gigabitethernet 0/5
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

Related Commands

Command	Description
debug ipv6 interface	Displays debugging information for IPv6 interfaces.
show ipv6 interface	Displays the status of interfaces configured for IPv6.

ipv6-address-pool

To specify a list of IPv6 address pools for allocating addresses to remote clients, use the **ipv6-address-pool** command in tunnel-group general-attributes configuration mode. To eliminate IPv6 address pools, use the **no** form of this command.

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool* [*...ipv6_address_pool6*]
no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool* [*...ipv6_address_pool6*]

Syntax Description

interface_name	(Optional) Specifies the interface to be used for the address pool.
ipv6_address_pool	Specifies the name of the address pool configured with the **ipv6 local pool** command. You can specify up to six local address pools.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

The IPv6 address-pool settings in the group-policy **ipv6-address-pools** command override the IPv6 address pool settings in the tunnel group **ipv6-address-pool** command.

The order in which you specify the pools is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

Examples

The following example entered in tunnel-group general-attributes configuration mode, specifies a list of IPv6 address pools for allocating addresses to remote clients for an IPsec remote access tunnel group test:

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
```

```
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

Related Commands

Command	Description
ipv6-address-pools	Configures the IPv6 address pools settings for the group policy, which override those settings for the tunnel group.
ipv6 local pool	Configures IP address pools to be used for VPN remote access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group	Configures a tunnel group.

ipv6-address-pools

To specify a list of up to six IPv6 address pools from which to allocate addresses to remote clients, use the **ipv6-address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

ipv6-address-pools value *ipv6_address_poll1* [*...ipv6_address_pool6*]
no ipv6-address-pools value *ipv6_address_poll1* [*...ipv6_address_pool6*]
ipv6-address-poolsnone
noipv6-address-poolsnone

Syntax Description

ipv6_address_pool	Specifies the names of the up to six IPv6 address pools configured with the **ipv6 local pool** command. Use spaces to separate the IPv6 address pool names.
none	Specifies that no IPv6 address pools are configured and disables inheritance from other sources of group policy.
value	Specifies a list of up to six IPv6 address pools from which to assign addresses.

Command Default

By default, the IPv6 address pools attribute is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

To configure IPv6 address pools, use the **ipv6 local pool** command.

The order in which you specify the pools in the **ipv6-address-pools** command is significant. The ASA allocates addresses from these pools in the order in which the pools appear in this command.

The **ipv6-address-pools none** command disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy. The **no ipv6-address-pools none** command removes the **ipv6-address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

Examples

The following example, entered in group-policy attributes configuration mode, configures an IPv6 address pool named firstipv6pool for use in allocating addresses to remote clients, then associates that pool with GroupPolicy1:

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# ipv6-
address-pools value firstipv6pool
ciscoasa(config-group-policy)#
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool to be used for VPN group policies.
clear configure group-policy	Clears all configured group policies.
show running-config group-policy	Shows the configuration for all group policies or for a particular group policy.

ipv6 dhcp client pd

To enable the DHCPv6 Prefix Delegation client, and name the prefix(es) obtained on an interface, use the **ipv6 dhcp client pd** command in interface configuration mode. To disable the client, use the **no** form of this command.

ipv6 dhcp client pd *name*
no ipv6 dhcp client pd *name*

Syntax Description

name Sets the name for this prefix. The name can be up to 200 characters. You will use this name when assigning an IP address to an interface using the prefix (**ipv6 address** *prefix_name*).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Enable the DHCPv6 Prefix Delegation client on one or more interfaces. The ASA obtains one or more IPv6 prefixes that it can subnet and assign to inside networks. Typically, the interface on which you enable the prefix delegation client obtains its IP address using the DHCPv6 address client; only other ASA interfaces use addresses derived from the delegated prefix.

This feature is not supported in clustering.

You cannot configure this feature on a management-only interface.

Examples

The following example configures the DHCPv6 address client and prefix delegation client on GigabitEthernet 0/0, then assigns addresses with the prefix on GigabitEthernet 0/1 and 0/2:

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.

Command	Description
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 dhcp client pd hint

To provide one or more hints about the delegated prefix you want to receive, use the **ipv6 dhcp client pd hint** command in interface configuration mode. To disable the client, use the **no** form of this command.

ipv6 dhcp client pd hint *ipv6_prefix / prefix_length*
no ipv6 dhcp client pd hint *ipv6_prefix / prefix_length*

Syntax Description

ipv6_prefix/prefix_length	Specifies the IPv6 prefix and length that you want to receive.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Typically you want to request a particular prefix length, such as ::/60, or if you have received a particular prefix before and want to ensure you get it again when the lease expires, you can enter the whole prefix as the hint. If you enter multiple hints (different prefixes or lengths), then it is up to the DHCP server which hint to honor, or whether to honor the hint at all.

Examples

The following example configures the DHCPv6 address client and prefix delegation client on GigabitEthernet 0/0, then assigns addresses with the prefix on GigabitEthernet 0/1 and 0/2:

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.

Command	Description
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 dhcp pool

To configure the IPv6 DHCP pool that contains the information you want the DHCPv6 server to provide to StateLess Address Auto Configuration (SLAAC) clients, use the **ipv6 dhcp pool** command in global configuration mode. To remove the pool, use the **no** form of this command.

ipv6 dhcp pool *pool_name*
no ipv6 dhcp pool *pool_name*

Syntax Description

pool_name	Specifies a name for the pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify this pool name when you enable the server. You can configure separate pools for each interface if you want, or you can use the same pool on multiple interfaces. After you enter the **ipv6 dhcp pool** command, you can configure one or more parameters to provide to the clients.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 dhcprelay enable

To enable DHCPv6 relay service on an interface, use the **ipv6 dhcprelay enable** command in global configuration mode. To disable the DHCPv6 relay service, use the **no** form of this command.

ipv6 dhcprelay enable *interface*
no ipv6 dhcprelay enable *interface*

Syntax Description

interface	Specifies the output interface for a destination.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command allows you to enable DHCPv6 relay service on an interface.When the service is enabled, incoming DHCPv6 messages from a client on the interface, which may have been relayed by another relay agent, are forwarded to all configured relay destinations through all configured outgoing links. For multiple context mode, you cannot enable DHCP relay service on an interface that is used by more than one context (that is, a shared interface).

Examples

The following example shows how to configure the DHCPv6 relay agent for a DHCPv6 server with an IP address of 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 on the ASA outside interface. Client requests are from the ASA inside interface, with a binding timeout value of 90 seconds.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

Command	Description
ipv6 dhcprelay server	Specifies the IPv6 DHCP server destination address to which client messages are forwarded.

Command	Description
ipv6 dhcprelay timeout	Sets the amount of time in seconds that is allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure.

ipv6 dhcp relay link-address

To configure one or more IPv6 addresses on an interface for use as the DHCPv6 relay link-address, use the **ipv6 dhcp relay link-address** command in interface configuration mode. To remove configured link-address values, use the **no** form of this command.

ipv6 dhcp relay link-address *ipv6_address*
no ipv6 dhcp relay link-address *ipv6_address*

Syntax Description

ipv6_address Specifies an IPv6 address to use as the link-address in DHCPv6 RELAY-FORWARD messages. The address must already be configured on the same interface. You can configure up to 5 IPv6 addresses.

Note
Use only static IPv6 address for *ipv6 dhcp relay link-address*. Do not use dynamic IPv6 addresses, like DHCP assigned address, EUI64, and the alike.

Command Default

If you do not configure a link-address, the ASA uses the first configured global unicast IPv6 address on the interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• input required	• input required	• Yes	• Yes	• input required

Command History

Release	Modification
9.24.10	This command was added.

Usage Guidelines

Use this command on the interface connected to DHCPv6 clients where DHCPv6 relay is enabled. Each configured link-address must already exist as an IPv6 address on the same interface. A DHCPv6 RELAY-FORWARD message can carry only one link address. When multiple link-addresses are configured, the ASA sends one RELAY-FORWARD packet for each configured link-address.

This behavior allows the DHCPv6 server to select an address pool based on prefix matching of the configured link-address.

If no link-address is configured, the ASA continues to use the first configured global unicast address on the interface. This behavior preserves backward compatibility with existing DHCPv6 relay deployments.

Up to 10 DHCPv6 servers can be configured by using the **ipv6 dhcprelay server** command.

Different DHCPv6 servers can behave differently when they receive multiple SOLICIT messages for the same client. Different DHCPv6 clients can behave differently when they receive multiple ADVERTISE messages.

No specific license is required for this feature.

Examples

The following example configures multiple IPv6 addresses on an interface and then specifies two of those addresses for use as DHCPv6 relay link-address values:

```
                ciscoasa(config)# interface Ethernet0/1
                ciscoasa(config-if)# ipv6 address 4001:1234:a:b::1/64
                ciscoasa(config-if)# ipv6 address 5001:1234:a:b::1/64
                ciscoasa(config-if)# ipv6 address 6001:1234:a:b::1/64
                ciscoasa(config-if)# ipv6 enable
                ciscoasa(config-if)# ipv6 dhcp relay link-address 5001:1234:a:b::1
6001:1234:a:b::1
                ciscoasa(config-if)# exit
                ciscoasa(config)# ipv6 dhcprelay server 3001:1234:a:b::3 inside
                ciscoasa(config)# ipv6 dhcprelay enable dmz
                ciscoasa(config)#
```

Related Commands

Command	Description
ipv6 dhcprelay enable	Enables DHCPv6 relay on an interface.
ipv6 dhcprelay server	Configures a DHCPv6 server for the relay agent.
show ipv6 dhcprelay binding	Displays DHCPv6 relay bindings.
show ipv6 dhcprelay statistics	Displays DHCPv6 relay statistics.
show ipv6 dhcprelay interface	Displays DHCPv6 relay interface configuration, including configured link-addresses.
debug ipv6 dhcprelay	Displays DHCPv6 relay debug information.

ipv6 dhcprelay server

To specify the IPv6 DHCP server destination address to which client messages are forwarded, use the **ipv6 dhcprelay server** command in global configuration mode. To remove the IPv6 DHCP server destination address, use the **no** form of this command.

ipv6 dhcprelay server *ipv6-address* [*interface*]
no ipv6 dhcprelay server *ipv6-address* [*interface*]

Syntax Description

interface	(Optional) Specifies the output interface for a destination.
ipv6-address	Can be a link-scoped unicast, multicast, site-scoped unicast, or global IPV6 address.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command enables you to specify the IPv6 DHCP server destination address to which client messages are forwarded. Client messages are forwarded to the destination address through the link to which the output interface is connected. If the specified address is a link-scoped address, then you must specify the interface. Unspecified, loopback, and node-local multicast addresses are not allowed as the relay destination. You can specify a maximum of ten servers per context.

Examples

The following example shows how to configure the DHCPv6 relay agent for a DHCPv6 server with an IP address of 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 on the ASA outside interface. Client requests are from the ASA inside interface, with a binding timeout value of 90 seconds.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

Command	Description
ipv6 dhcprelay enable	Enables IPv6 DHCP relay service on an interface.

Command	Description
ipv6 dhcprelay timeout	Sets the amount of time in seconds that is allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure.

ipv6 dhcprelay timeout

To set the amount of time in seconds that are allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure, use the **ipv6 dhcprelay timeout** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6dhcprelaytimeout*seconds*
noipv6dhcprelaytimeout*seconds*

Syntax Description

seconds	Sets the number of seconds that are allowed for DHCPv6 relay address negotiation. Valid values range from 1 to 3600.

Command Default

The default is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command allows you to set the amount of time in seconds that are allowed for responses from the DHCPv6 server to pass to the DHCPv6 client through the relay binding structure.

Examples

The following example shows how to configure the DHCPv6 relay agent for a DHCPv6 server with an IP address of 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 on the ASA outside interface. Client requests are from the ASA inside interface, with a binding timeout value of 90 seconds.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

Related Commands

Command	Description
ipv6 dhcprelay server	Specifies the IPv6 DHCP server destination address to which client messages are forwarded.
ipv6 dhcprelay enable	Specifies the IPv6 DHCP server destination address to which client messages are forwarded.

ipv6 dhcp server

For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature, configure the DHCPv6 stateless server using the **ipv6 dhcp server** command in interface configuration mode. To disable the DHCP server, use the **no** form of this command.

ipv6 dhcp server *pool_name*
no ipv6 dhcp server *pool_name*

Syntax Description

pool_name	Sets the name of the IPv6 pool configured with the **ipv6 dhcp pool** command. This pool includes information that you want to provide to clients on a given interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
```

```
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.

Command	Description
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

ipv6 eigrp

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

ipv6 eigrp *as_number*
no ipv6 eigrp *as_number*

Syntax Description

as_number	Autonomous system number. Valid values are from 1 to 65535.

Command Default

EIGRP is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was introduced.

Examples

The following example shows how to configure EIGRP for ipv6 on an interface:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 eigrp 12 ?
```

Related Commands

Command	Description
clear ipv6 eigrp	Clears the entries from EIGRP for IPv6 routing tables.
show ipv6 eigrp	Displays the EIGRP router configuration mode commands in the running configuration. Displays information about interfaces configured with IPv6 EIGRP.

ipv6 hello-interval eigrp

To specify the interval between EIGRP hello packets sent on an interface, use the **hello-interval** command in address-family interface configuration mode or service-family interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

ipv6 hello-interval eigrp *as_number seconds*
no ipv6 hello-interval eigrp *as_number seconds*

Syntax Description

as_number	Specifies the autonomous system number of the EIGRP routing process.
seconds	Specifies the interval between hello packets that are sent on the interface. Valid values are from 1 to 65535 seconds.

Command Default

The EIGRP hello interval is 60 seconds for low-speed Non-broadcast multiple access (NBMA) networks and 5 seconds for all other networks.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will occur. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the EIGRP hello interval to 10 seconds:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hello-interval eigrp 1 10
```

Related Commands

Command	Description
hold-time	Configures the EIGRP hold time advertised in hello packets.

ipv6 hold-time eigrp

To specify the hold time advertised by the ASA in EIGRP hello packets, use the **hold-time** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

ipv6 hold-time eigrp *as_number seconds*
no ipv6 hold-time eigrp *as_number seconds*

Syntax Description

as_number	The autonomous system number of the EIGRP routing process.
seconds	Specifies the hold time, in seconds. Valid values are from 1 to 65535 seconds.

Command Default

The EIGRP hello interval is 180 seconds for low-speed Non-broadcast multiple access (NBMA) networks and 15 seconds for all other networks.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

This value is advertised in the EIGRP hello packets sent by the ASA. The EIGRP neighbors on that interface use this value to determine the availability of the ASA. If they do not receive a hello packet from the ASA during the advertised hold time, the EIGRP neighbors will consider the ASA to be unavailable.

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If the ASA does not receive a hello packet within the specified hold time, routes through this neighbor are considered unavailable.

Increasing the hold time delays route convergence across the network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hello-interval eigrp 1 10
ciscoasa(config-if)# ipv6 hold-time eigrp 1 30
```

Related Commands

Command	Description
ipv6 hello-interval eigrp	Specifies the interval between EIGRP hello packets sent on an interface.

ipv6 router eigrp

To start an IPv6 EIGRP routing process and configure parameters for that process, use the **ipv6 router eigrp** command in global configuration mode. To disable EIGRP routing, use the **no** form of this command.

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

Syntax Description

as-number	Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information. Valid values are from 1 to 65535.

Command Default

EIGRP routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

The **router eigrp** command creates an EIGRP routing process or enters router configuration mode for an existing EIGRP routing process.

Use the following router configuration mode commands to configure the EIGRP routing processes:

- **default-metric**—Define the default metrics for routes redistributed into the EIGRP routing process.
- **distribute-list**—Filter the networks received and sent in routing updates.
- **eigrp router-id**—Creates a fixed router ID.
- **neighbor**—Statically define an EIGRP neighbor.
- **passive-interface**—Configure an interface to act as a passive interface.
- **redistribute**—Redistribute routes from other routing processes into EIGRP.

Examples

The following example shows how to enter the configuration mode for the EIGRP routing process with the autonomous system number 125:

```
ciscoasa(config)# ipv6 router eigrp 125
ciscoasa(config-router)# eigrp router-id 10.1.1.1
```

Related Commands

Command	Description
clear configure eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

ipv6 split-horizon eigrp

To reenable EIGRP split horizon, use the **ipv6 split-horizon eigrp** command in address-family interface configuration mode. To disable EIGRP split horizon, use the **no** form of this command.

ipv6 split-horizon eigrp *as_number*
no ipv6 split-horizon eigrp *as_number*

Syntax Description

as_number	The autonomous system number of the EIGRP routing process.

Command Default

EIGRP for IPv6 split horizon is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

To negate the split horizon feature, you can explicitly specify the **no ipv6 split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

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

Examples

The following example disables EIGRP split-horizon on interface gigabitEthernet 0/0:

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# no ipv6 split-horizon eigrp 1
```

Related Commands

Command	Description
ipv6 router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

ipv6 summary-address eigrp

To configure a summary for EIGRP on a specific interface, use the **ipv6 summary-address eigrp** command in interface configuration mode. To remove the summary address, use the **no** form of this command.

ipv6 summary-address eigrp *as_number ipv6 address* [*admin-distance*]
no ipv6 summary-address eigrp *as_number ipv6 address*

Syntax Description

as_number	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.
ipv6 address	The summary IPv6 address to apply on the interface.
admin-distance	(Optional) The administrative distance of the summary route. Valid values are from 0 to 255.

Command Default

The defaults are as follows:

- EIGRP for IPv6 automatically summarizes routes to the network level, even for a single host route. No summary addresses are predefined.
- The administrative distance of EIGRP for IPv6 summary routes is 5.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.20(1)	This command was added.

Usage Guidelines

By default, EIGRP summarizes subnet routes to the network level. Use the **no auto-summary** command to disable automatic route summarization. Using the **summary-address** command lets you manually define subnet route summaries on a per-interface basis.

Examples

The following example configures route summary:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 summary-address eigrp 1 4001::1/64 ?
interface mode commands/options:
  <1-255>  Administrative distance
```

Related Commands

Command	Description
auto-summary	Automatically creates summary addresses for the EIGRP routing process.

ipv6 enable

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

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—
Global configuration	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface, while also enabling the interface for IPv6 processing.

The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

Related Commands

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

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

ipv6 enforce-eui64

To enforce the use of modified EUI-64 format interface identifiers in IPv6 addresses on a local link, use the **ipv6 enforce-eui64** command in global configuration mode. To disable modified EUI-64 address format enforcement, use the **no** form of this command.

ipv6 enforce-eui64 *if_name*
no ipv6 enforce-eui64 *if_name*

Syntax Description

if_name	Specifies the name of the interface, as designated by the **nameif** command, for which you are enabling modified EUI-64 address format enforcement.

Command Default

Modified EUI-64 format enforcement is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

When this command is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the modified EUI-64 format. If the IPv6 packets do not use the modified EUI-64 format for the interface identifier, the packets are dropped and the following syslog message is generated:

```
%ASA-3-325003: EUI-64 source address check failed.
```

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

The modified EUI-64 format interface identifier is derived from the 48-bit link-layer (MAC) address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower three bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64-bit interface ID of 02E0:B6FF:FE01:3B7A.

Examples

The following example enables modified EUI-64 format enforcement for IPv6 addresses received on the inside interface:

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address on an interface.
ipv6 enable	Enables IPv6 on an interface.

ipv6 icmp

To configure ICMP access rules for an interface, use the **ipv6 icmp** command in global configuration mode. To remove an ICMP access rule, use the **no** form of this command.

ipv6 icmp { **permit** | **deny** } { *ipv6-prefix / prefix-length* | **any** | **host** *ipv6-address* } [*icmp-type*] *if-name*
no ipv6 icmp { **permit** | **deny** } { *ipv6-prefix / prefix-length* | **any** | **host** *ipv6-address* } [*icmp-type*] *if-name*

Syntax Description

any	Keyword specifying any IPv6 address. An abbreviation for the IPv6 prefix ::/0.
deny	Prevents the specified ICMP traffic on the selected interface.
host	Indicates that the address refers to a specific host.
icmp-type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	The name of the interface, as designated by the **nameif** command, to which the access rule applies.
ipv6-address	The IPv6 address of the host sending ICMPv6 messages to the interface.
ipv6-prefix	The IPv6 network that is sending ICMPv6 messages to the interface.

permit	Allows the specified ICMP traffic on the selected interface.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Command Default

If no ICMP access rules are defined, all ICMP traffic is permitted.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

ICMP in IPv6 functions the same as ICMP in IPv4. ICMPv6 generates error messages, such as ICMP destination unreachable messages and informational messages like ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process and path MTU discovery.

The minimum MTU allowed on an IPv6 enabled interface is 1280 bytes; however, if IPsec is enabled on the interface, the MTU value should not be set below 1380 because of the overhead of IPsec encryption. Setting the interface below 1380 bytes may result in dropped packets.

If there are no ICMP rules defined for an interface, all IPv6 ICMP traffic is permitted.

If there are ICMP rules defined for an interface, then the rules are processed in order on a first-match basis followed by an implicit deny all rule. For example, if the first matched rule is a permit rule, the ICMP packet is processed. If the first matched rule is a deny rule, or if the ICMP packet did not match any rule on that interface, then the ASA discards the ICMP packet and generates a syslog message.

For this reason, the order that you enter the ICMP rules is important. If you enter a rule denying all ICMP traffic from a specific network, and then follow it with a rule permitting ICMP traffic from a particular host on that network, the host rule will never be processed. The ICMP traffic is blocked by the network rule. However, if you enter the host rule first, followed by the network rule, the host ICMP traffic will be allowed, while all other ICMP traffic from that network is blocked.

The **ipv6 icmp** command configures access rules for ICMP traffic that terminates at the ASA interfaces. To configure access rules for pass-through ICMP traffic, see the **ipv6 access-list** command.

Examples

The following example denies all ping requests and permits all packet-too-big messages (to support path MTU discovery) at the outside interface:

```
ciscoasa(config)# ipv6 icmp deny any echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

The following example permits host 2000:0:0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

Command	Description
ipv6 access-list	Configures access lists.

ipv6 local pool

To configure an IPv6 address pool, use the **ipv6 local pool** command in global configuration mode. To delete the pool, use the **no** form of this command.

ipv6 local pool *pool_name ipv6_address / prefix_length number_of_addresses*
no ipv6 local pool *pool_name ipv6_address / prefix_length number_of_addresses*

Syntax Description

ipv6_address	Specifies the starting IPv6 address for the pool.
number_of_addresses	Range: 1-16384.
pool_name	Specifies the name to assign to this IPv6 address pool.
prefix_length	Range: 0-128.

Command Default

By default, the IPv6 local address pool is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	IPv6 local pool for the cluster pool in the **ipv6 address** command to support ASA clustering was added.

Usage Guidelines

For VPN, to assign IPv6 local pools, use either the **ipv6-local-pool** command in the tunnel group or the **ipv6-address-pools** command (note the "s" on this command) in the group policy. The ipv6-address-pools setting in the group policy overrides the ipv6-address-pools setting in the tunnel group.

Examples

The following example configures an IPv6 address pool named firstipv6pool for use in allocating addresses to remote clients:

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

Related Commands

Command	Description
ipv6-address-pool	Associates IPv6 address pools with a VPN tunnel group policy.
ipv6-address-pools	Associates IPv6 address pools with a VPN group policy.
clear configure ipv6 local pool	Clears all configured IPv6 local pools.
show running-config ipv6	Shows the configuration for IPv6.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection, use the **ipv6 nd dad attempts** command in interface configuration mode. To return to the default number of duplicate address detection messages sent, use the **no** form of this command.

ipv6 nd dad attempts *value*
no ipv6 nd dad attempts *value*

Syntax Description

value A number from 0 to 600. Entering 0 disables duplicate address detection on the specified interface. Entering 1 configures a single transmission without follow-up transmissions. The default value is 1 message.

Command Default

The default number of attempts is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses. The frequency at which the neighbor solicitation messages are sent is configured using the **ipv6 nd ns-interval** command.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state.

Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up. An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

Note While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Examples

The following example configures 5 consecutive neighbor solicitation messages to be sent when duplicate address detection is being performed on the tentative unicast IPv6 address of the interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

The following example disables duplicate address detection on the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd managed-config-flag

To configure the ASA to set the managed address config flag in the IPv6 router advertisement packet, use the **ipv6 nd managed config-flag** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ipv6 nd managed-config-flag
no ipv6 managed-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The IPv6 autoconfiguration client host can use this flag to indicate that it must use the stateful address configuration protocol (DHCPv6) to obtain addresses in addition to the derived stateless autoconfiguration address.

Examples

The following example sets the managed address config flag in the IPv6 router advertisement packet for the interface GigabitEthernet 0/0:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

Related Commands

Command	Description
ipv6 nd other-config-flag	Configures the ASA to set the other config flag in the IPv6 router advertisement packet.

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ns-interval *value*
no ipv6 nd ns-interval [*value*]

Syntax Description

value	The interval between IPv6 neighbor solicitation transmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds. The default value is 1000 milliseconds.

Command Default

The default is 1000 milliseconds between neighbor solicitation transmissions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

This value will be included in all IPv6 router advertisements sent out this interface.

Examples

The following example configures an IPv6 neighbor solicitation transmission interval of 9000 milliseconds for GigabitEthernet 0/0:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

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

ipv6 nd other-config-flag

To configure the ASA to set the other config flag in the IPv6 router advertisement packet, use the **ipv6 nd other-config-flag** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ipv6 nd other-config-flag
no ipv6 other-config-flag

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The IPv6 autoconfiguration client host can use this flag to indicate that it must use the stateful address configuration protocol (DHCPv6) to obtain non-address configuration information such as DNS server information.

Examples

The following example sets the other config flag in the IPv6 router advertisement packet for the interface GigabitEthernet 0/0:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

Related Commands

Command	Description
ipv6 nd managed-config-flag	Configures the ASA to set the managed address config flag in the IPv6 router advertisement packet.

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix *ipv6-prefix* | *prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]
no ipv6 nd prefix *ipv6-prefix* | *prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

Syntax Description

at *valid-date preferred-date*	The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* .
default	Default values are used.
infinite	(Optional) The valid lifetime does not expire.
ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal format using 16-bit values between colons.
no-advertise	(Optional) Indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration. For the **default** prefix, this setting only applies to on-link prefixes. Off-link prefixes will still be advertised unless you specify **no-advertise** for a specific off-link prefix.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is not used for on-link determination.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with the **infinite** keyword. The default is 604800 (7 days).
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
valid-lifetime	The amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with the **infinite** keyword. The default is 2592000 (30 days).

Command Default

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the "onlink" and "autoconfig" flags set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

The **default** keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

When onlink is “on” (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is “on” (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Examples

The following example includes the IPv6 prefix 2001:200::/35, with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds in router advertisements sent out on the specified interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra dns-search-list

To set the DNS Search List (DNSSL) option to advertise a list of search domains to IPv6 clients, use the **ipv6 nd ra dns-search-list** command in interface configuration mode. To remove the server, use the **no** form of this command.

ipv6 nd ra dns-search-list domain *domain_name* [**lifetime** *lifetime_value*]
no ipv6 nd ra dns-search-list domain *domain_name* [**lifetime** *lifetime_value*]

Syntax Description

domain *domain_name*	The domain name to append to unqualified names.
lifetime *lifetime_value*	(Optional) The maximum time, in seconds, that the domain will be used, between 200 and 4294967295. If you set the value to 0, the entry will not be used. If you set the value to 4294967295, the entry will never expire. The default is 3 x the maximum RA interval (see the **ipv6 nd ra-interval** command). The value must be greater than or equal to the RA interval.

Command Default

3 x the **ipv6 nd ra-interval** (600 seconds).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.24(1)	This command was added.

Usage Guidelines

This option is useful for clients that use SLAAC instead of DHCPv6 for their addressing. Note that if you enabled the prefix delegation client on the ASA, you can alternatively pass along the DNS domain that the ASA received using the ASA's DHCPv6 stateless server.

You can set up to 5 domains.

Examples

The following example configures two domains to advertise to SLAAC clients:

```
ciscoasa(config)# interface ethernet 1/2
ciscoasa(config-if)# ipv6 nd ra dns-search-list domain cisco.com
ciscoasa(config-if)# ipv6 nd ra dns-search-list domain example.com
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
ipv6 nd ra dns server	Sets the Recursive DNS Server (RDNSS) option to advertise a list of DNS servers to IPv6 clients.
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra dns server

To set the Recursive DNS Server (RDNSS) option to advertise a list of DNS servers to IPv6 clients, use the **ipv6 nd ra dns server** command in interface configuration mode. To remove the server, use the **no** form of this command.

ipv6 nd ra dns server *dns_server_ipv6_address* [*lifetime_value*]
no ipv6 nd ra dns server *dns_server_ipv6_address* [*lifetime_value*]

Syntax Description

dns_server_ipv6_address	The address of DNS server.
lifetime_value	(Optional) The maximum time, in seconds, that the DNS server will be used for name resolution, between 200 and 4294967295. If you set the value to 0, the entry will not be used. If you set the value to 4294967295, the entry will never expire. The default is 3 x the maximum RA interval (see the **ipv6 nd ra-interval** command). The value must be greater than or equal to the RA interval.

Command Default

3 x the **ipv6 nd ra-interval** (600 seconds).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.24(1)	This command was added.

Usage Guidelines

This option is useful for clients that use SLAAC instead of DHCPv6 for their addressing. Note that if you enabled the prefix delegation client on the ASA, you can alternatively pass along the DNS server information that the ASA received using the ASA's DHCPv6 stateless server.

You can set up to 8 DNS servers.

Examples

The following example configures four DNS servers to advertise to SLAAC clients:

```
ciscoasa(config)# interface ethernet 1/2
ciscoasa(config-if)# ipv6 nd ra dns server 2620:119:35::35
ciscoasa(config-if)# ipv6 nd ra dns server 2620:119:53::53
ciscoasa(config-if)# ipv6 nd ra dns server 2606:4700:4700::1111
ciscoasa(config-if)# ipv6 nd ra dns server 2606:4700:4700::1001
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
ipv6 nd ra dns-search-list	Sets the DNS Search List (DNSSL) option to advertise a list of search domains to IPv6 clients.
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval [**msec**] *value*
no ipv6 nd ra-interval [[**msec**] *value*]

Syntax Description

msec	(Optional) indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is seconds.
value	The interval between IPv6 router advertisement transmissions. Valid values range from 3 to 1800 seconds, or from 500 to 1800000 milliseconds if the **msec** keyword is provided. The default is 200 seconds.

Command Default

200 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the ASA is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime

To configure the “router lifetime” value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*
no ipv6 nd ra-lifetime [*seconds*]

Syntax Description

seconds	The validity of the ASA as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the ASA should not be considered a default router on the selected interface.

Command Default

1800 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The “router lifetime” value is included in all IPv6 router advertisements sent out an interface. The value indicates the usefulness of the ASA as a default router on this interface.

Setting the value to a non-zero value to indicates that the ASA should be considered a default router on this interface. The non-zero value for the “router lifetime” value should not be less than the router advertisement interval.

Setting the value to 0 indicates that the ASA should not be considered a default router on this interface.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *value*
no ipv6 nd reachable-time [*value*]

Syntax Description

value The amount of time, in milliseconds, that a remote IPv6 node is considered reachable. Valid values range from 0 to 3600000 milliseconds. The default value is 0.

When 0 is used for the *value* argument, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.

Command Default

Zero milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

The configured time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

To see the reachable time used by the ASA, including the actual value when this command is set to 0, use the **show ipv6 interface** command to display information about the IPv6 interface, including the ND reachable time being used.

Examples

The following example configures an IPv6 reachable time of 1700000 milliseconds for the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

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

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Command Default

Router advertisements are automatically sent on LAN interfaces if IPv6 unicast routing is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on the selected interface:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra
```

Related Commands

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

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static entry from the neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6_address if_name mac_address*
no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

Syntax Description

if_name	The internal or external interface name designated by the **nameif** command.
ipv6_address	The IPv6 address that corresponds to the local data link address.
mac_address	The local data line (hardware MAC) address.

Command Default

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the **copy** command is used to store the configuration.

Use the **show ipv6 neighbor** command to view static entries in the IPv6 neighbor discovery cache.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

The following example adds a static entry for the an inside host with an IPv6 address of 3001:1::45A and a MAC address of 0002.7D1A.9472 to the neighbor discovery cache:

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

ipv6 ospf

To enable the OSPFv3 interface configuration for IPv6, use the **ipv6 ospf** command in global configuration mode. To disable the OSPFv3 interface configuration for IPv6, use the **no** form of this command.

ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]
no ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

Syntax Description

cost	Explicitly specifies the cost of sending a packet on an interface.
database-filter	Filters outgoing LSAs to an OSPFv3 interface.
dead-interval *seconds*	Sets the time period in seconds for which hello packets must not be seen before neighbors indicate that the router is down. The value must be the same for all nodes on the network and can range from 1 to 65535. The default is four times the interval set by the **ipv6 ospf hello-interval** command.
flood-reduction	Specifies the flood reduction of LSAs to the interface.
hello-interval *seconds*	Specifies the interval in seconds between hello packets sent on the interface. The value must be the same for all nodes on a specific network and can range from 1 to 65535. The default interval is 10 seconds for Ethernet interfaces and 30 seconds for non-broadcast interfaces.
mtu-ignore	Disables the OSPF MTU mismatch detection when DBD packets are received. OSPF MTU mismatch detection is enabled by default.
neighbor	Configures OSPFv3 router interconnections to non-broadcast networks.
network	Sets the OSPF network type to a type other than the default, which depends on the network type.
priority	Sets the router priority, which helps determine the designated router for a network. Valid values range from 0 to 255.
process-id	Specifies the OSPFv3 process to be enabled. Valid values range from 1 to 65535.
retransmit-interval *seconds*	Specifies the time in seconds between LSA retransmissions for adjacencies that belong to the interface. The time must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds. The default is 5 seconds.
transmit-delay *seconds*	Sets the estimated time in seconds to send a link-state update packet on the interface. Valid values range from 1 to 65535 seconds. The default is 1 second.

Command Default

All IPv6 addresses are included by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You must enable an OSPFv3 routing process before you can create an OSPFv3 area.

Examples

The following example enables OSPFv3 interface configuration:

```
ciscoasa(config)# ipv6 ospf 3
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf area

To create an OSPFv3 area for IPv6, use the **ipv6 ospf area** command in global configuration mode. To disable the OSPFv3 area configuration for IPv6, use the **no** form of this command.

ipv6 ospf area [*area-num*] [**instance**]
no ipv6 ospf area [*area-num*] [**instance**]

Syntax Description

area-num	Specifies the OSPFv3 area to be enabled.
instance	Specifies the area instance ID that is to be assigned to an interface.

Command Default

All IPv6 addresses are included by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You must configure OSPFv3 routing on each interface separately. An interface can have only one OSPFv3 area, and OSPFv3 for the ASA supports only one instance per interface. Each interface uses a different area instance ID. The area instance ID only affects the receipt of OSPF packets, and applies to normal OSPF interfaces and virtual links.

Examples

The following example enables OSPFv3 interface configuration:

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf cost

To explicitly specify the cost of sending a packet on an interface, use the **ipv6 ospf cost** command in interface configuration mode. To reset the cost of sending a packet on an interface to the default value, use the **no** form of this command.

ipv6 ospf cost *interface-cost*
no ipv6 ospf cost *interface-cost*

Syntax Description

interface-cost	Specifies an unsigned integer value expressed as the link-state metric, which can range from 1 to 65535.

Command Default

The default cost is based on the bandwidth.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to explicitly specify the packet cost for an interface.

Examples

The following example sets the packet cost to 65:

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf database-filter all out

To filter outgoing LSAs to an OSPFv3 interface, use the **ipv6 ospf databse-filter all out** command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the **no** form of this command.

ipv6 ospf database-filter all out
no ipv6 ospf database-filter all out

Syntax Description

This command has no arguments or keywords.

Command Default

All outgoing LSAs are flooded to the interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to filter outgoing LSAs to an OSPFv3 interface.

Examples

The following example filters outgoing LSAs to the specified interface:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf dead-interval

To set the time period for which hello packets must not be seen before neighbors declare that the router is down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval *seconds*

Syntax Description

seconds	Specifies the interval in seconds. The value must be the same for all nodes in the network. Valid values range from 1 to 65535.

Command Default

The default is four times the interval that is set by the **ipv6 ospf hello-interval** command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the interval during which hello packets are not seen before neighbors notify that the router is down.

Examples

The following example sets the dead interval to 60:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf encryption

To specify the encryption type for an interface, use the **ipv6 ospf encryption** command in interface configuration mode. To remove the encryption type for an interface, use the **no** form of this command.

ipv6 ospf encryption { **ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null** }
no ipv6 ospf encryption { **ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null** }

Syntax Description

authentication-algorithm	Specifies the encryption algorithm to be used. Valid values are one of the following: • **md5**—Enables message digest 5 (MD5). • **sha1**—Enables SHA-1.
encryption-algorithm	Specifies the encryption algorithm to be used with ESP . . Valid values are the following: • **aes-cdc**—Enables AES-CDC encryption. • **3des**—Enables 3DES encryption. • **des**—Enables DES encryption. • **null**—Specifies ESP with no encryption.
esp	Specifies the encapsulating security payload (ESP).
ipsec	Specifies the IP security protocol.
key	Specifies the number used in the calculation of the message digest. When MD5 authentication is used, the key must be 32 hexadecimal digits (16 bytes) long. When SHA-1 authentication is used, the key must be 40 hexadecimal digits (20 bytes) long.
key-encryption-type	(Optional) Specifies the key encryption type, which can be one of the following values: • **0**—The key is not encrypted. • **7**—The key is encrypted.
null	Overrides area authentication.
spi *spi*	Specifies the security policy index (SPI) value. The *spi* value must be a number from 256 to 4294967295, which is entered as a decimal.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the encryption type for an interface.

Examples

The following example enables SHA-1 encryption on the interface:

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf flood-reduction

To specify the flood reduction of LSAs to the interface, use the **ipv6 ospf flood-reduction** command in interface configuration mode. To remove the flood reduction of LSAs to the interface, use the **no** form of this command.

ipv6 ospf flood-reduction
no ipv6 ospf flood-reduction

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the flood reduction of LSAs to an interface.

Examples

The following example enables flood reduction of LSAs to the interface:

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.

Command	Description
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf hello-interval

To set the time period for which hello packets must not be seen before neighbors declare that the router is down, use the **ipv6 ospf dead-interval** command in interface configuration mode. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval *seconds*

Syntax Description

seconds	Specifies the interval in seconds. The value must be the same for all nodes in the network. Valid values range from 1 to 65535.

Command Default

The default interval is 10 seconds if you are using Ethernet and 30 seconds if you are using non-broadcast.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the interval during which hello packets are not seen before neighbors notify that the router is down.

Examples

The following example sets the dead interval to 60:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf mtu-ignore

To disable OSPFv3 maximum transmission unit (MTU) mismatch detection when the ASA receives database descriptor (DBD) packets, use the **ipv6 ospf mtu-ignore** command in interface configuration mode. To reset the MTU mismatch detection when the ASA receives DBD packets to the default, use the **no** form of this command.

ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Command Default

OSPFv3 MTU mismatch detection is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to disable OSPFv3 MTU mismatch detection when the ASA receives DBD packets.

Examples

The following example disables OSPFv3 MTU mismatch detection when the ASA receives DBD packets:

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6 ospf neighbor

To configure OSPFv3 router interconnections to nonbroadcast networks, use the **ipv6 ospf neighbor** command in interface configuration mode. To remove a configuration, use the **no** form of this command.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]
no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

Syntax Description

cost *number*	(Optional) Assigns a cost to the neighbor in the form of an integer from 1 to 65535. Neighbors with no specific cost configured assume the cost of the interface, based on the **ipv6 ospf cost** command.
database-filter	(Optional) Filters outgoing link-state advertisements (LSAs) to an OSPF neighbor.
ipv6-address	Link-local IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal format using 16-bit values between colons.
poll-interval *seconds*	(Optional) A number value that represents the poll interval time in seconds. RFC 2328 recommends that this value be much larger than the hello interval. The default is 120 seconds (two minutes). This keyword does not apply to point-to-multipoint interfaces.
priority *number*	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IPv6 prefix specified. The default is 0.

Command Default

The default depends on the network type.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	•	•		—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure OSPFv3 router interconnections to nonbroadcast networks.

Examples

The following example configures an OSPFv3 neighboring router:

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6 ospf network

To configure the OSPFv3 network type to a type other than the default, use the **ipv6 ospf network** command in interface configuration mode. To return to the default type, use the **no** form of this command.

ipv6 ospf network { **broadcast** | **point-to-point non-broadcast** }
no ipv6 ospf network { **broadcast** | **point-to-point non-broadcast** }

Syntax Description

broadcast	Sets the network type to broadcast.
point-to-point non-broadcast	Sets the network type to point-to-point non-broadcast.

Command Default

The default depends on the network type.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure the OSPFv3 network type to a type that is different from the default.

Examples

The following example sets the OSPFv3 network to a broadcast network:

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6 ospf priority

To set the router priority, which helps determine the designated router for a specified network, use the **ipv6 ospf priority** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *number-value*
no ipv6 ospf priority *number-value*

Syntax Description

number-value	Sets the number value that specifies the priority of the router. Valid values range from 0 to 255.

Command Default

The default priority is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to set the priority of the router.

Examples

The following example sets the priority of the router to 4:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf retransmit-interval	Specifies the time between LSA retransmissions for adjacencies that belong to the interface.

ipv6 ospf retransmit-interval

To specify the time between LSA retransmissions for adjacencies that belong to the interface, use the **ipv6 ospf retransmit-interval** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *seconds*
no ipv6 ospf retransmit-interval *seconds*

Syntax Description

seconds	Specifies the time in seconds between retransmissions. The interval must be greater than the expected round-trip delay between any two routers on the attached network. Valid values range from 1 to 65535 seconds.

Command Default

The default is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to specify the time between LSA retransmissions for adjacencies that belong to the interface.

Examples

The following example sets the retransmission interval to 8 seconds:

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

Related Commands

Command	Description
ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6 ospf transmit-delay

To set the estimated time that is required to send a link-state update packet on the interface, use the **ipv6 ospf transmit-delay** command in interface configuration mode. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *seconds*
no ipv6 ospf transmit-delay *seconds*

Syntax Description

seconds	Specifies the time in seconds that is required to send a link-state update. Valid values range from 1 to 65535 seconds.

Command Default

The default is 1 second.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to set the estimated time that is required to send a link-state update packet on the interface.

Examples

The following example sets the transmission delay to 3 seconds:

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

Related Commands

Command	Description
clear ipv6 ospf	Deletes all IPv6 settings in the OSPFv3 routing process.
ipv6 ospf priority	Determines the designated router for a specified network.

ipv6-prefix

To configure the IPv6 prefix for the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **ipv6-prefix** command in MAP domain basic mapping rule configuration mode. Use the **no** form of this command to remove the prefix.

ipv6-prefix *ipv6_prefix / prefix_length*
no ipv6-prefix *ipv6_prefix / prefix_length*

Syntax Description

ipv6_prefix/prefix_length	The IPv6 prefix defines the address pool for the customer edge (CE) device's IPv6 address. Specify an IPv6 prefix and prefix length, which is normally 64, but cannot be less than 8. You cannot use the same IPv6 prefix in different MAP domains.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain basic mapping rule configuration mode	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The IPv6 prefix defines the address pool for the CE device's IPv6 address. MAP translates IPv6 packets back to IPv4 only if the packets have a destination address with this prefix and a source address with the IPv6 prefix defined in the default mapping rule, and is within the right port range. Any IPv6 packets sent to the CE device from other addresses are simply processed as IPv6 traffic without MAP translation. Packets from the MAP source/destination pools, but with out-of-range ports, are simply dropped.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule
```

```
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

ipv6 prefix-list

To create an entry in an IPv6 prefix list, use the **ipv6 prefix-list** command in global configuration mode. To delete the entry, use the **no** form of this command.

ipv6 prefix-list *list-name* [**seq** *seq-number*] { **deny** *ipv6-prefix* | *prefix-length* | **description** *text* } [**ge** *ge-value*] [**le** *le-value*]
no ipv6 prefix-list *list-name*

Syntax Description

list-name	Name of the prefix list. Cannot be the same name as an existing access list. **Note** The name cannot be ‘detail’ or ‘summary’, because they are keywords.
seq *seq-number*	(Optional) Sequence number of the prefix list entry being configured.
deny	Denies networks that match the condition.
permit	Permits networks that match the condition.
ipv6-prefix	The IPv6 network assigned to the specified prefix list. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
description *text*	A description of the prefix list that can be up to 80 characters in length.
ge *ge-value*	(Optional) Specifies a prefix length greater than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the lowest value of a range of the length (the "from" portion of the length range).
le *le-value*	(Optional) Specifies a prefix length less than or equal to the *ipv6-prefix*/*prefix-length* arguments. It is the highest value of a range of the length (the "to" portion of the length range).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Related Commands

Command	Description
show ipv6 prefix-list	Displays IPv6 prefix lists.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 route

To add an IPv6 route to the IPv6 routing table, use the **ipv6 route** command in global configuration mode. To remove an IPv6 default route, use the **no** form of this command.

ipv6 route *if_name ipv6-prefix* | *prefix-length ipv6-address* [*administrative-distance* | **tunneled**]
no ipv6 route *if_name ipv6-prefix* | *prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

Syntax Description

administrative-distance	(Optional) The administrative distance of the route. The default value is 1, which gives static routes precedence over any other type of routes except connected routes.
if_name	The name of the interface for which the route is being configured.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network.
ipv6-prefix	The IPv6 network that is the destination of the static route. This argument must be in the form documented in RFC 2373, in which the address is specified in hexadecimal format using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
tunneled	(Optional) Specifies the route as the default tunnel gateway for VPN traffic.

Command Default

By default, the administrative distance is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	Support for transparent firewall mode was added.

Usage Guidelines

Use the **show ipv6 route** command to view the contents of the IPv6 routing table.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the ASA that cannot

be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled**option:

- Do not enable unicast RPF (**ip verify reverse-path** command) on the egress interface of the tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route. Doing so causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, or SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes. These inspection engines ignore the tunneled route.

You cannot define more than one default route with the **tunneled**option; ECMP for tunneled traffic is not supported.

Examples

The following example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1 with an administrative distance of 110:

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

Related Commands

Command	Description
debug ipv6 route	Displays debugging messages for IPv6 routing table updates and route cache updates.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6 router ospf

To create an OSPFv3 routing process and enter IPv6 router configuration mode, use the **ipv6 router ospf** command in global configuration mode.

ipv6 router ospf *process-id*

Syntax Description

process-id	Specifies the internal identification, which is locally assigned and can be a positive integer from 1 to 65535. The number used is the number that is assigned administratively when you enable the OSPFv3 for IPv6 routing process.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **ipv6 router ospf** command is the global configuration command for OSPFv3 routing processes running on the ASA. After you enter the **ipv6 router ospf** command, the command prompt appears as (config-rtr)#, indicating that you are in IPv6 router configuration mode.

When using the **no ipv6 router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no ipv6 router ospf** command terminates the OSPFv3 routing process specified by its *process-id* argument. You assign the *process-id* value locally on the ASA. You must assign a unique value for each OSPFv3 routing process. You can use a maximum of two processes.

Use the **ipv6 router ospf** command in IPv6 router configuration mode to configure OSPFv3 routing processes with the following OSPFv3-specific options:

- **area**—Configures OSPFv3 area parameters. Supported parameters include the area ID as a decimal value from 0 to 4294967295 and the area ID in the IP address format of **A.B.C.D**.
- **default**—Sets a command to its default value. The **originate** parameter distributes the default route.
- **default-information**—Controls distribution of default information.
- **distance**—Defines the OSPFv3 route administrative distance based on the route type. Supported parameters include the administrative distance with values from 1 to 254 and **ospf** for the OSPF distance.

- **exit—**Exits IPv6 router configuration mode.
- **ignore**—Suppresses the sending of syslog messages with the **lsa** parameter when the router receives a link-state advertisement (LSA) for Type 6 Multicast OSPF (MOSPF) packets.
- **log-adjacency-changes**—Configures the router to send a syslog message when an OSPFv3 neighbor goes up or down. With the **detail** parameter, all state changes are logged.
- **passive-interface**—Suppresses routing updates on an interface with the following parameters:
  - **GigabitEthernet**—Specifies the GigabitEthernet IEEE 802.3z interface.
  - **Management**—Specifies the management interface.
  - **Port-channel**—Specifies the Ethernet channel of an interface.
  - **Redundant**—Specifies the redundant interface.
  - **default**—Suppresses routing updates on all interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain into another according to the following parameters:
  - **connected**—Specifies connected routes.
  - **ospf**—Specifies OSPF routes.
  - **static**—Specifies static routes.
- **router-id**—Creates a fixed router ID for a specified process with the following parameters:
  - **A.B.C.D**—Specifies the OSPF router ID in IP address format.
  - **cluster-pool**—Configures an IP address pool when Layer 3 clustering is configured.
- **summary-prefix**—Configures IPv6 address summaries with valid values from 0 to 128. The **X:X:X:X::X/** parameter specifies the IPv6 prefix.
- **timers—**Adjusts routing timers with the following parameters:
  - **lsa**—Specifies OSPF LSA timers.
  - **pacing**—Specifies OSPF pacing timers.
  - **throttle**—Specifies OSPF throttle timers.

Examples

The following example enables an OSPFv3 routing process and enters IPv6 router configuration mode:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
clear ipv6 ospf	Removes all IPv6 settings in the OSPFv3 routing process.

Command	Description
debug ospfv3	Provides debugging information for troubleshooting OSPFv3 routing processes.

ipv6-split-tunnel-policy

To set a IPv6 split tunneling policy, use the **ipv6-split-tunnel-policy** command in group-policy configuration mode. To remove the ipv6-split-tunnel-policy attribute from the running configuration, use the **no** form of this command.

ipv6-split-tunnel-policy { **tunnelall** | **tunnelspecified** | **excludespecified** }
no ipv6-split-tunnel-policy

Syntax Description

excludespecified	Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel.
ipv6-split-tunnel-policy	Indicates that you are setting rules for tunneling traffic.
tunnelall	Specifies that no traffic goes in the clear or to any other destination than the ASA. Remote users reach Internet networks through the corporate network and do not have access to local networks.
tunnelspecified	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's Internet service provider.

Command Default

IPv6 split tunneling is disabled by default, which is **tunnelall**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

IPv6 split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable IPv6 split tunneling.

This enables inheritance of a value for IPv6 split tunneling from another group policy.

IPv6 split tunneling lets a remote-access VPN client conditionally direct packets over an IPsec or SSL IPv6 tunnel in encrypted form, or to a network interface in cleartext form. With IPv6 split-tunneling enabled, packets

not bound for destinations on the other side of the IPsec or SSL VPN tunnel endpoint do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies IPv6 split tunneling policy to a specific network.

Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-split-
tunnel-policy tunnelspecified
```

Related Commands

Command	Description
split-tunnel-network-list none	Indicates that no access list exists for split tunneling. All traffic travels across the tunnel.
split-tunnel-network-list value	Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not.

ipv6-vpn-address-assign

To specify a method for assigning IPv6 addresses to remote access clients, use the **ipv6-vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all configured VPN address assignment methods from the ASA, user the **no** version of this command. without arguments.

ipv6-vpn-addr-assign { **aaa** | **local** }
no ipv6-vpn-addr-assign { **aaa** | **local** }

Syntax Description

aaa	The ASA retrieves addresses from an external or internal (LOCAL) AAA (authentication, authorization, and accounting) server on a per-user basis. If you are using an authentication server that has IP addresses configured, we recommend using this method.
local	The ASA distributes IPv6 addresses from internally configured address pools.

Command Default

Both the AAA and local VPN address assignment options are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.
9.5(2)	Support for multiple context mode was added.

Usage Guidelines

The ASA can use either the AAA or local methods for assigning IPv6 addresses to remote access clients. If you configure more than one address assignment method, the ASA searches each of the options until it finds an IPv6 address.

Examples

The following example shows how to configure AAA as the address assignment method.

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

The following example shows how to configure the use of a local address pool for the address assignment method.

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool to be used for VPN group policies.
show running-config group-policy	Shows the configuration for all group policies or for a particular group policy.
vpn-addr-assign	Specifies a method for assigning IPv4 addresses to remote access clients.

ipv6-vpn-filter

To specify the name of the IPv6 ACL to use for VPN connections, use the **ipv6-vpn-filter** command in group-policy configuration or username configuration mode. To remove the ACL, including a null value created by issuing the **ipv6-vpn-filter none** command, use the **no** form of this command.

ipv6-vpn-filter { **value** *IPV6-ACL-NAME* | **none** }
no ipv6-vpn-filter

Syntax Description

none	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *IPV6-ACL-NAME*	Provides the name of the previously configured access list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	The **ipv6-vpn-filter** command was deprecated. Use the **vpn-filter** command to configure unified filters with either IPv4 and IPv6 entries. This IPv6 filter is only used if there are no IPv6 entries in the access list specified by the **vpn-filter** command.
9.1(4)	The **ipv6-vpn-filter** command has been disabled, only the "no" form of the command is allowed. Use **vpn-filter** command to configure unified filters for IPv4 and IPv6 entries. If this command is mistakenly used to specify IPv6 ACLs the connection is terminated.

Usage Guidelines

Clientless SSL VPN does not use the ACL defined in the **ipv6-vpn-filter** command.

The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **ipv6-vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **ipv6-vpn-filter** command to apply those ACLs.

Examples

The following example shows how to set a filter that invokes an access list named ipv6_acl_vpn for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-vpn-filter value ipv6_acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
vpn-filter	Specifies the names of an IPv4 or IPv6 ACL to use for VPN connections.

ip verify reverse-path

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip verify reverse-path interface *interface_name*
no ip verify reverse-path interface *interface_name*

Syntax Description

interface_name	The interface on which you want to enable Unicast RPF.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

Normally, the ASA only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the ASA to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the ASA, the ASA routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the ASA can use the default route to satisfy Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the ASA uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the ASA drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the ASA drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.

- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure that they arrived on the same interface used by the initial packet.

Examples

The following example enables Unicast RPF on the outside interface:

```
ciscoasa(config)# ip verify reverse-path interface outside
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the configuration set using the **ip verify reverse-path** command.
clear ip verify statistics	Clears the Unicast RPF statistics.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the configuration set using the **ip verify reverse-path** command.

ipv6 unnumbered

To borrow or inherit an IPv6 address from an interface (for example, a loopback interface), use the **ipv6 unnumbered** command in the interface configuration mode. To stop inheriting an ip address from an interface, use the **no** form of this command.

ipv6 unnumbered *interface-name*
no ipv6 unnumbered

Syntax Description

interface-name	Specifies the name of an interface to inherit the IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface Configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.19(1)	This command was added.

Usage Guidelines

The `ipv6 unnumbered` command is used to inherit the IPv6 address of the selected *`interface`* as the address for the current interface.

Examples

The following example borrows the IPv6 address from the loopback interface and uses it for the VTI tunnel interface:

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ipv6 unnumbered loopback1
```

Related Commands

Command	Description
ip unnumbered *interface-name*	Inherits the IP address of the specified interface.
interface loopback *loopback-number*	Creates a loopback interface.