show ipv – show ir

show ipv6 access-list

To display the IPv6 access list, use the **show ipv6 access-list** command in privileged EXEC mode. The IPv6 access list determines what IPv6 traffic can pass through the ASA.

show ipv6 access-list [*id* [*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*]]

Syntax Description

any	(Optional) An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	(Optional) IPv6 address of a specific host. When provided, only the access rules for the specified host are displayed.
id	(Optional) The access list name. When provided, only the specified access list is displayed.
source-ipv6-prefix /prefix-length	(Optional) IPv6 network address and prefix. When provided, only the access rules for the specified IPv6 network are displayed.

Command Default

Displays all IPv6 access lists.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	IPv6 access rules were incorporated into the **access-list** command, so this command is no longer meaningful.

Usage Guidelines

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

This command shows only those access lists configured using the **ipv6 access-list** command. In ASA 9.0(1), IPv6 access control was integrated into the same **access-list** structure as IPv4. Thus, in systems running software versions starting with 9.0(1), the **show ipv6 access-list** command is no longer meaningful.

Examples

The following is sample output from the **show ipv6 access-list** command. It shows IPv6 access lists named inbound, tcptraffic, and outbound.

```
ciscoasa# show ipv6 access-list
```

```
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

Related Commands

Command	Description
ipv6 access-list	Creates an IPv6 access list.

show ipv6 dhcp

To show DHCPv6 information, use the **show ipv6 dhcp** command in privileged EXEC mode.

show ipv6 dhcp [**client** [**pd**] **statistics | interface** [*interface_name* [**statistics**]] **| ha statistics | server statistics | pool** [*pool_name*]]

Syntax Description

client	Shows DHCPv6 client statistics and shows the output of the number of messages sent and received.
pd	Shows DHCPv6 Prefix Delegation client statistics.
statistics	Shows statistics.
interface	Shows DHCPv6 information for all interfaces. If the interface is configured for DHCPv6 stateless server configuration (see **ipv6 dhcp server**), this command lists the DHCPv6 pool that is being used by the server. If the interface has DHCPv6 address client or Prefix Delegation client configuration, this command shows the state of each client and the values received from the server.
interface_name	(Optional) For a specific interface, you can show message statistics for the DHCP server or client.
ha	Shows the transaction statistics between failover units, including how many times the DUID information was synced between the units.
server	Shows the DHCPv6 stateless server statistics.
pool	Shows DHCPv6 pools.
pool_name	(Optional) Shows the specified 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

If you do not specify any arguments, this command displays the device DUID that is being used by the DHCPv6 client or server.

Examples

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

```
ciscoasa# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

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

```
ciscoasa# show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
  SIP server address: 2001::abcd:1
  SIP server domain name: sip.xyz.com
```

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

```
ciscoasa# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool
GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD
Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
```

```
      Information refresh time: 0
```

The following is sample output from the **show ipv6 dhcp interface outside** command:

```
ciscoasa# show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode
 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
   Preference: 0
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

The following is sample output from the **show ipv6 dhcp interface outside statistics** command:

```
ciscoasa# show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:
Protocol Exchange Statistics:
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0
Error and Failure Statistics:
 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
DHCPV6 Client address statistics:
Protocol Exchange Statistics:
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0
Error and Failure Statistics:
 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp client statistics** command:

```
ciscoasa# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0
Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp client pd statistics** command:

```
ciscoasa# show ipv6 dhcp client pd statistics
Protocol Exchange Statistics:
 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0
Error and Failure Statistics:
 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp server statistics** command:

```
ciscoasa# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0
Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp ha statistics** command:

```
ciscoasa# show ipv6 dhcp ha statistics
DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0
```

```
DHCPv6 HA error statistics:
  Send errors:                          0
```

The following is sample output from the **show ipv6 dhcp ha statistics** command on a standby unit:

```
ciscoasa# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1
DHCPv6 HA error statistics:
  Send errors:                          0
```

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.

show ipv6 dhcprelay binding

To display the relay binding entries created by the relay agent, use the **show ipv6 dhcprelay binding** command in privileged EXEC mode.

show ipv6 dhcprelay binding

Syntax Description

This command has no keywords or variables.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 dhcprelay binding** command allows you to check the relay binding entries that the relay agent has created.

Examples

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

```
ciscoasa# show ipv6 dhcprelay binding
1 in use, 2 most used
Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds
Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
 the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
 60 seconds.
There will be limit of 1000 bindings for each context.
```

Related Commands

Command	Description
show ipv6 dhcprelay statistics	Shows the IPv6 DHCP relay agent information.

show ipv6 dhcprelay statistics

To display the IPv6 DHCP relay agent statistics, use the **show ipv6 dhcprelay statistics** command in privileged EXEC mode.

show ipv6 dhcprelay statistics

Syntax Description

This command has no keywords or variables.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 dhcprelay statistics** command allows you to view IPv6 DHCP relay agent information.

Examples

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

```
ciscoasa# show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                    1
  ADVERTISE                                  2
  REQUEST                                    1
  CONFIRM                                    1
  RENEW                                    496
  REBIND                                     0
  REPLY                                    498
  RELEASE                                    0
  DECLINE                                    0
  RECONFIGURE                                0
  INFORMATION-REQUEST                        0
  RELAY-FORWARD                            499
  RELAY-REPLY                              500
Relay Errors:
  Malformed message:                         0
  Block allocation/duplication failures:     0
  Hop count limit exceeded:                  0
  Forward binding creation failures:         0
  Reply binding lookup failures:             0
  No output route:                           0
  Conflict relay server route:               0
```

```
  Failed to add server NP rule:                0
  Unit or context is not active:               0
Total Relay Bindings Created:                498
```

Related Commands

Command	Description
show ipv6 dhcprelay binding	Shows the relay binding entries created by the relay agent.

show ipv6 general-prefix

To show all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes, use the **show ipv6 general-prefix** command in privileged EXEC mode.

show ipv6 general-prefix

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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

To see the preferred lifetime of the prefix assigned by the DHCPv6 Server, use the **show ipv6 general-prefix** command. When you use Prefix Delegation, you must set the ASA IPv6 neighbor discovery router advertisement interval to be much lower than the preferred lifetime of the prefix assigned by the DHCPv6 Server to prevent IPv6 traffic interruption. For example, if the DHCPv6 server sets the preferred Prefix Delegation lifetime to 300 seconds, you should set the ASA RA interval to be 150 seconds. To set the ASA RA interval, see the **ipv6 nd ra-interval** command; the default is 200 seconds.

Examples

The following is sample output from the **show ipv6 general-prefix** command that shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes ("Consumer List"):

```
ciscoasa# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
    BGP network command         1
    inside (Address command)    1
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.

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

show ipv6 icmp

To display the ICMPv6 access rules configured on all interfaces, use the **show ipv6 icmp** command in privileged EXEC mode.

show ipv6 icmp

Syntax Description

This command has no arguments or variables.

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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

ICMPv6 rules control ICMPv6 traffic to device interfaces. They do not control through-the-box traffic. You would use these rules to control which addresses could send ICMPv6 commands to an interface (for example, pings), and which types of ICMPv6 commands could be sent. Use the **show ipv6 icmp** command to view these rules.

Examples

The following is sample output from the **show ipv6 icmp** command.

```
ciscoasa show ipv6 icmp
ipv6 icmp permit any inside
```

Related Commands

Command	Description
ipv6 icmp	Configures IPv6 ICMP management access rules.

show ipv6 interface

To display the status of interfaces configured for IPv6, use the **show ipv6 interface** command in privileged EXEC mode.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

Syntax Description

brief	Displays a brief summary of IPv6 status and configuration for each interface.
if_name	(Optional) The internal or external interface name, as designated by the **nameif** command. The status and configuration for only the designated interface is shown.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool. The prefix is the network portion of the IPv6 address.

Command Default

Displays all IPv6 interfaces.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.10(1)	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces.
9.10(1)	Support to indicate supervisor non-association for the Firepower 2100/4100/9300 was added.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show interface** command, except that it is IPv6-specific. If the interface hardware is usable, the interface is marked >*up* . If the interface can provide two-way communication, the line protocol is marked >*up* . For Firepower 2100/4100/9300 devices, to indicate supervisor is not associated with IPv6 interfaces, “not associated with Supervisor” is displayed along the line protocol status.

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

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

```
ciscoasa# show ipv6 interface outside
```

```
interface ethernet0 "outside" is up, line protocol is up "not associated with Supervisor"
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
ciscoasa# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

For Firepower 2100/4100/9300 devices, to indicate supervisor is not associated with IPv6 interfaces, "not associated with Supervisor" is displayed along the line protocol status. The following is sample output from the **show ipv6 interface** command. It shows the characteristics of an interface which has generated a prefix from an address.

```
ciscoasa# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar
AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

To display IPv6 address pool information, use the **show ipv6 local pool** command in privileged EXEC mode.

show ipv6 local pool interface *pool_name*

Syntax Description

pool_name	The name of the address pool. Enter ? to see a list of pools.

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
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use this command to view the contents of IPv6 address pools created using the **ipv6 local pool** command. These pools are used with remote access VPN and clustering. Use the **ip local pool** command to view IPv4 address pools.

Examples

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

```
ciscoasa# show ipv6 local pool test-ipv6-pool

IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15
Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
```

```
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool.

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counter information, use the **show ipv6 mld traffic** command in privileged EXEC mode.

show ipv6 mld traffic

Syntax Description

This command has no keywords or variables.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)	This command was added.

Usage Guidelines

The **show ipv6 mld traffic** command allows you to check if the expected number of MLD messages have been received and sent.

The following information is provided by the **show ipv6 mld traffic** command:

- Elapsed time since counters cleared—The amount of time since the counters were cleared.
- Valid MLD Packets—The number of valid MLD packets that are received and sent.
- Queries—The number of valid queries that are received and sent.
- Reports—The number of valid reports that are received and sent.
- Leaves—The number of valid leaves received and sent.
- Mtraee packets—The number of multicast trace packets that are received and sent.
- Errors—The types of errors and the number of errors that have occurred.

Examples

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

```
ciscoasa# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
     Received      Sent
```

```
Valid MLD Packets      1      3
Queries      1      0
Reports       0      3
Leaves      0      0
Mtrace packets      0     0
Errors:
Malformed Packets      0
Martian source      0
Non link-local source 0
Hop limit is not equal to 1 0
```

Related Commands

Command	Description
clear ipv6 mld traffic	Resets all MLD traffic counters.

show ipv6 neighbor

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbor** command in privileged EXEC mode.

show ipv6 neighbor [*if_name* | *address*]

Syntax Description

address	(Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
if_name	(Optional) Displays cache information for the supplied interface name, as configured by the **nameif** command only.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The following information is provided by the **show ipv6 neighbor** command:

- IPv6 Address—The IPv6 address of the neighbor or interface.
- Age—The time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- Link-layer Addr—The MAC address. If the address is unknown, a hyphen (-) is displayed.
- State—The state of the neighbor cache entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.

The following are possible states for dynamic entries in the IPv6 neighbor discovery cache:

- INCMP—(Incomplete) Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.

- REACH—(Reachable) Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.
- STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.
- DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.
- PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
- ????—Unknown state.

The following are possible states for static entries in the IPv6 neighbor discovery cache:

- INCMP—(Incomplete) The interface for this entry is down.
- REACH—(Reachable) The interface for this entry is up.
- Interface

The interface from which the address was reachable.

Examples

The following is sample output from the **show ipv6 neighbor** command when entered with an interface:

```
ciscoasa# show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

The following is sample output from the **show ipv6 neighbor** command when entered with an IPv6 address:

```
ciscoasa# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.

show ipv6 ospf

To display general information about OSPFv3 routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*]

Syntax Description

area_id	(Optional) Shows information about a specified area only.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 ospf** command lists the following settings:

- Event logging
- Router type
- Redistribution route type
- SPF schedule delay
- Hold time between two consecutive SPFs
- Wait time between two consecutive SPFs
- Minimum LSA interval
- Minimum LSA arrival

Examples

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

```
ciscoasa# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

Related Commands

Command	Description
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).
show ipv6 ospf database	Shows lists of information related to the OSPFv3 database for a specific router.

show ipv6 ospf border-routers

To display the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR), use the **show ipv6 ospf border-routers** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **border-routers**

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 ospf border-routers** command lists the following settings:

- Intra-area route
- Inter-area route
- IPv6 address
- Interface type
- Area ID
- SPF number

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
ciscoasa# show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
```

```
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf database	Shows lists of information related to the OSPFv3 database for a specific router.

show ipv6 ospf database

To display lists of information related to the OSPFv3 database for a specific router, use the **show ipv6 ospf database** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external | inter-area prefix | inter-area-router | network | nssa-external | router | area | as | ref-lsa** [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] **| self-originate**] [**internal**] [**database-summary**]

Syntax Description

adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. The router ID must be in the form documented in RFC 2740, in which the address is specified in hexadecimal using 16-bit values between colons.
area	(Optional) Displays information only about area LSAs.
area_id	(Optional) Displays information about a specified area only.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
database-summary	(Optional) Displays how many of each type of LSA exists for each area in the database and the total.
destination-router-id	(Optional) Displays information about a specified destination router only.
external	(Optional) Displays information only about the external LSAs.
interface	Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface name.
internal	(Optional) Displays information only about the internal LSAs.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
link	(Optional) Displays information about link LSAs. When it follows the **unknown** keyword, the **link** keyword filters link-scope LSAs.
link-state-id	(Optional) Specifies an integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
network	(Optional) Displays information about network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix *ipv6-prefix*	(Optional) Displays the link-local IPv6 address of the neighbor. The IPv6 prefix must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
ref-lsa	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information about router LSAs.
self-originate	(Optional) Displays only self-originated LSAs from the local router.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The various forms of the command provide information about different OSPFv3 LSAs.

Examples

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

```
ciscoasa# show ipv6 ospf database
            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)
                Router Link States (Area 0)
ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Router Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3
            Link (Type-8) Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
```

```
            Intra Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf events

To display OSPFv3 internal event information, use the **show ipv6 ospf events** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **events** [*type*]

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type	(Optional) A list of the event types you want to see. If you do not specify one or more types, you see all events. You can filter on the following types: • **generic**—Generic events. • **interface**—Interface state change events. • **lsa**—LSA arrival and LSA generation events. • **neighbor**—Neighbor state change events. • **reverse**—Show events in reverse order. • **rib**—Router Information Base update, delete and redistribution events. • **spf**—SPF scheduling and SPF run events.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

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

```
ciscoasa# show ipv6 ospf events
OSPFv3 Router with ID (10.1.3.2) (Process ID 10)
```

```
  1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,
 Seq# 80000008, Age 1, Area 10
  3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004, Age
  0, Area 10
  4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,
 Age 0, Area 10
  5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
  6 Jul 9  18:41:18.902: Starting External processing in area 10
  7 Jul 9  18:41:18.902: Starting External processing
  8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
  9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
 10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
 11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
 12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
 13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
 14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
 15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0, Adv-Rtr
  50.100.168.192
 16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf flood-list

To display a list of OSPFv3 LSAs waiting to be flooded over an interface, use the **show ipv6 ospf flood-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface-number	Specifies the interface number over which the LSAs are flooded.
interface-type	Specifies the interface type over which the LSAs are flooded.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to display OSPFv3 packet pacing information.

Examples

The following is sample output from the **show ipv6 ospf flood-list** command:

```
ciscoasa# show ipv6 ospf flood-list
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971
 Interface FastEthernet0/0, Queue length 0
 Interface ATM3/0, Queue length 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf graceful-restart

To display information about OSPFv3 graceful-restart, use the **show ipv6 ospf** graceful-restart command in privileged EXEC mode.

show ipv6 ospf graceful-restart

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Examples

The following is sample output from the **show ipv6 ospf graceful-restart** command:

```
ciscoasa# show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.

show ipv6 ospf interface

To display OSPFv3-related interface information, use the **show ipv6 ospf interface** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type-number	(Optional) Specifies the interface type and number.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to display overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Examples

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

```
ciscoasa# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
```

```
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf neighbor

To display OSPFv3 neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
detail	(Optional) Displays all neighbors information in detail.
interface-type interface-number	(Optional) Specifies the interface type and number.
neighbor-id	(Optional) Specifies the neighbor ID.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to display detailed information for OSPFv3 neighbors by interface.

Examples

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

```
ciscoasa# show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4       1    FULL/  -        00:00:31    14              POS4/0
172.16.3.3       1    FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5       1    FULL/  -        00:00:33    13              ATM3/0
```

The following is sample output from the **show ipv6 ospf neighbor detail** command:

```
Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf request-list

To display a list of all LSAs that have been requested by a router, use the **show ipv6 ospf request-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface	(Optional) Specifies the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Specifies the list of all LSAs requested by the router on this interface from this neighbor.
neighbor	(Optional) Specifies the list of all LSAs requested by the router from this neighbor.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to list all LSAs that a router requests.

Examples

The following is sample output from the **show ipv6 ospf request-list** command:

```
ciscoasa# show ipv6 ospf request-list
            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
```

```
2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf retransmission-list

To display a list of all LSAs that have been waiting to be resent, use the **show ipv6 ospf retransmission-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface	(Optional) Specifies the list of all LSAs waiting to be resent on this interface.
interface-neighbor	(Optional) Specifies the list of all LSAs waiting to be resent for this interface from this neighbor.
neighbor	(Optional) Specifies the list of all LSAs waiting to be resent for this neighbor.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to list all LSAs that are waiting to be resent.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
ciscoasa# show ipv6 ospf retransmission-list
        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf statistic

To display various OSPFv3 statistics, use the **show ipv6 ospf statistic** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **statistic** [**detail**]

Syntax Description

detail	(Optional) Specifies detailed SPF information, including the trigger points.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to list the number of times SPF was executed, the reasons, and the duration.

Examples

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

```
ciscoasa# show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times
SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)
SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
```

```
SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
     0      0      0      0      0      0      0 0
RIB manipulation time (in msec):
RIB Update    RIB Delete
             0             0
LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
Change record R N L
LSAs changed 5
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
50.100.168.192/2(N)
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPFv3 process, use the **show ipv6 ospf summary-prefix** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **summary-prefix**

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show a list of all summary address redistribution information that has been configured under an OSPFv3 process.

Examples

The following is sample output from the **show ipv6 ospf summary-prefix** command:

```
ciscoasa# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf timers

To display OSPFv3 timers information, use the **show ipv6 ospf timers** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **timers** [**lsa-group | rate-limit**]

Syntax Description

lsa-group	(Optional) Specifies OSPFv3 LSA group information.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
rate-limit	(Optional) Specifies OSPFv3 LSA rate limit information.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show LSA information that has been configured under an OSPFv3 process.

Examples

The following is sample output from the **show ipv6 ospf timers lsa-group** command:

```
ciscoasa# show ipv6 ospf timers lsa-group
OSPFv3 Router with ID (10.10.13.101) (Process ID 1)
Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548
Failure Head 0, Last 0 LSA group failure logged
            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)
Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
```

```
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546
Failure Head 0, Last 0 LSA group failure logged
```

The following is sample output from the **show ipv6 ospf timers rate-limit** command:

```
ciscoasa# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf traffic

To display OSPFv3 traffic-related statistics for currently available interfaces, use the **show ipv6 ospf traffic** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the name of the interface (for example, interface GigabitEthernet0/0). Use this option to segregate traffic to a specific interface.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show OSPFv3 traffic-related information for available interfaces.

Examples

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

```
ciscoasa# show ipv6 ospf 10 traffic inside
Interface inside
Last clearing of interface traffic counters never
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid                       0 0
  RX Hello                      1232 53132
  RX DB des                       27 896
  RX LS req                        3 216
  RX LS upd                       28 2436
  RX LS ack                       14 1064
  RX Total                      1304 57744
  TX Failed                        0 0
  TX Hello                       753 32072
  TX DB des                       27 1056
```

```
TX LS req                        2 92
TX LS upd                        9 1128
TX LS ack                       15 900
TX Total                       806 35248
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf virtual-links

To displayparameters and the current state of OSPFv3 virtual links, use the **show ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

show ipv6 ospf virtual-links

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
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show parameters and the current state of OSPFv3 virtual links.

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command:

```
ciscoasa# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 prefix-list

To display information about configured IPv6 prefix lists, use the **show ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [**summary | detail**] [*policy list_name* [**seq** *sequence_number* | *network/length* [**longer | first-match**]]]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.
summary	(Optional) Show additional summarized statistical information.
detail	(Optional) Show additional summarized statistical information plus prefix list entries.
seq *sequence_number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
network/length [**longer** | **first-match**]	(Optional) Displays all entries in the specified prefix list that use this network address and prefix length (in bits). You can add these keywords to modify the match: • **longer**—Displays all entries of the specified prefix list that match or are more specific than the given network/length. • **first-match**—Displays the first entry of the specified prefix list that matches the given network/length.

Command Default

If you do not specify a prefix list name, this command shows all of the prefix lists. If you do not include other keywords, the output shows the prefix list entries only.

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
User EXEC or Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Prefix lists are used in routing as matching criteria for route maps and policy lists.

Examples

The following is sample output from the **show ipv6 prefix-list** command.

```
ciscoasa(config)# show ipv6 prefix-list

ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

The following is an example of summarized output.

```
ciscoasa(config)# show ipv6 prefix-list summary

Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

The following is an example of detailed output.

```
ciscoasa(config)# show ipv6 prefix-list detail

Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
   seq 5 permit 2001:db8:0:cd30::/64 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
ipv6 prefix-list	Configures IPv6 prefix lists.

show ipv6 route management-only

To display the contents of the IPv6 routing table, use the **show ipv6 route** command in privileged EXEC mode. The management-only keyword displays routes in the IPv6 management routing table.

show ipv6 route management-only [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]

Syntax Description

managment-only	Displays routes in the IPv6 management routing table.
cluster	(Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number in a cluster.
failover	(Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number.
interface	(Optional) Displays IPv6 interface-specific routes.
ospf	(Optional) Displays OSPFv3 routes.
summary	(Optional) Displays IPv6 route summaries.

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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for the **failover, cluster, ospf, interface,** and **summary** keywords was added.
9.5(1)	Support for the management routing table feature was added.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show route** command, except that the information is IPv6-specific.

The following information appears in the IPv6 routing table:

- Codes—Indicates the protocol that derived the route. Values are as follows:
- C—Connected
- L—Local

- S—Static
- R—RIP derived
- B—BGP derived
- I1—ISIS L1—Integrated IS-IS Level 1 derived
- I2—ISIS L2—Integrated IS-IS Level 2 derived
- IA—ISIS interarea—Integrated IS-IS interarea derived
- fe80::/10—Indicates the IPv6 prefix of the remote network.
- [0/0]—The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
- via ::—Specifies the address of the next router to the remote network.
- inside—Specifies the interface through which the next router to the specified network can be reached.

Note The **clustering** and **failover** keywords do not appear unless these features are configured on the ASA.

Examples

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

```
ciscoasa# show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

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

```
ciscoasa# show ipv6 route failover
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired
```

```
O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

The following is sample output from the **show ipv6 route cluster** command on the master unit:

```
ciscoasa/LB1/master(config)# show ipv6 route cluster
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired
OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

The following is sample output from the **show ipv6 route cluster** command on the slave unit during a role change:

```
ciscoasa/LB2/slave(config)# cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
ciscoasa/LB2/slave(config)#
ciscoasa/LB2/master(config)#
ciscoasa/LB2/master(config)# show ipv6 route cluster
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs
OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

Related Commands

Command	Description
debug ipv6 route	Displays debugging messages for IPv6 routing table updates and route cache updates.
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 routers

To display IPv6 router advertisement information received from on-link routers, use the **show ipv6 routers** command in privileged EXEC mode.

show ipv6 routers [*if_name*]

Syntax Description

if_name (Optional) The internal or external interface name, as designated by the **nameif** command, that you want to display information about.

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an interface name:

```
ciscoasa# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

Command	Description
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command in privileged EXEC mode.

show ipv6 traffic

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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **clear ipv6 traffic** command to clear the traffic counters.

Examples

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

```
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent
ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
```

```
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert
UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output
TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

Related Commands

Command	Description
clear ipv6 traffic	Clears IPv6 traffic counters.