

show n – show o

- show nac-policy, on page 2
- show nameif, on page 4
- show nat, on page 6
- show nat divert-table, on page 9
- show nat pool, on page 12
- show nat proxy-arp, on page 16
- show ntp associations, on page 18
- show ntp status, on page 22
- show nve, on page 24
- show object, on page 27
- show object-group, on page 30
- show ospf, on page 36
- show ospf border-routers, on page 38
- show ospf database, on page 39
- show ospf events, on page 43
- show ospf flood-list, on page 45
- show ospf interface, on page 47
- show ospf neighbor, on page 49
- show ospf nsf, on page 51
- show ospf request-list, on page 52
- show ospf retransmission-list, on page 53
- show ospf rib, on page 55
- show ospf statistics, on page 56
- show ospf summary-address, on page 58
- show ospf traffic, on page 59
- show ospf virtual-links, on page 61

show nac-policy

To show the NAC policy usage statistics and the assignment of NAC policies to group policies, use the **show nac-policy** command in privileged EXEC mode.

show nac-policy [*nac-policy-name*]

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to display usage statistics.

Command Default

If you do not specify a name, the CLI lists all NAC policy names along with their respective statistics.

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
8.0(2)	This command was added.

Examples

The following example shows the data for the NAC policies named framework1 and framework2:

```
ciscoasa(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

The first line of each NAC policy indicates its name and type (nac-framework). The CLI shows the text "is not in use" next to the policy type if the policy is not assigned to any group policies. Otherwise, the CLI displays the usage data for the group policy. Table 10-1 explains the fields in the **show nac-policy** command.

Table 1: show nac-policy Command Fields

Field	Description
applied session count	Cumulative number of VPN sessions to which this ASA applied the NAC policy.
applied group-policy count	Cumulative number of group polices to which this ASA applied the NAC policy.

Field	Description
group-policy list	List of group policies to which this NAC policy is assigned. In this case, the usage of a group policy does not determine whether it appears in this list; if the NAC policy is assigned to a group policy in the running configuration, then the group policy appears in this list.

Related Commands

clear nac-policy	Resets the NAC policy usage statistics.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
show vpn-session_summary.db	Displays the number IPSec, Cisco WebVPN, and NAC sessions.

show nameif

To view the interface name set using the **nameif** command, use the **show nameif** command in privileged EXEC mode.

show nameif [*physical_interface* [*.subinterface*] | *mapped_name* | **zone**]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit ethernet0/1** . See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
zone	(Optional) Shows the zone names.

Command Default

If you do not specify an interface, the ASA shows all interface names.

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.
9.3(2)	The **zone** keyword was added.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context. The output for this command shows only the mapped name in the Interface column.

Examples

The following is sample output from the **show nameif** command:

```
ciscoasa# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

See the following output for the **show nameif zone** command:

```
ciscoasa# show nameif zone
Interface                Name                    zone-name       Security
GigabitEthernet0/0       inside-1                inside-zone      100
GigabitEthernet0/1.21    inside                  inside-zone      100
GigabitEthernet0/1.31    4                                          0
GigabitEthernet0/2       outside                 outside-zone    0
Management0/0            lan                                        0
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show nat

To display statistics of NAT policies, use the **show nat** command in privileged EXEC mode.

show nat [**interface** *name*] [*ip_addr* [*mask*] | { **object | object-group** } *name*] [**translated** [**interface** *name*] { *ip_addr* [*mask*] | { **object | object-group** } *name* }] [**detail**]

Syntax Description

detail	(Optional) Includes more verbose expansion of the object fields.
interface *name*	(Optional) Specifies the source interface.
ip_addr [*mask*]	(Optional) Specifies an IP address and subnet mask.
object *name*	(Optional) Specifies a network object or service object.
object-group *name*	(Optional) Specifies a network object group
translated	(Optional) Specifies the translated parameters.

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
8.3(1)	This command was added.
9.0(1)	Support for IPv6 traffic, as well as translations between IPv4 and IPv6 were added.

Usage Guidelines

Use the **show nat** command to show runtime representation of the NAT policy. Use the **detail** optional keyword to expand the object and view the object values. Use the additional selector fields to limit the **show nat** command output.

Examples

The following is sample output from the **show nat** command:

```
ciscoasa# show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
```

```
   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
ciscoasa# show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
 1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

The following is sample output from the **show nat detail** command between IPv6 and IPv4:

```
ciscoasa# show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

Starting with version 9.16, Section 0 shows the system-defined NAT rules, which are needed for the system to function properly. These show rules for internal interfaces, such as nlp_int_tap. These rules take priority over all other rules. You cannot add or change rules in Section 0.

```
ciscoasa(config)# show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source dynamic nlp_client_0_0.0.0.0_17proto53_intf3 interface
 destination static nlp_client_0_ipv4_2 nlp_client_0_ipv4_2 service nlp_client_0_17svc53_1
 nlp_client_0_17svc53_1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.99.11.7/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Origin: udp destination eq domain , Translated: udp destination eq domain
2 (nlp_int_tap) to (inside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.99.11.7/24
3 (nlp_int_tap) to (inside) source dynamic nlp_client_0_ipv6_::_17proto53_intf3 interface
ipv6  destination static nlp_client_0_ipv6_4 nlp_client_0_ipv6_4 service
nlp_client_0_17svc53_3 nlp_client_0_17svc53_3
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::2/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Origin: udp destination eq domain , Translated: udp destination eq domain
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.

show nat divert-table

To display statistics of NAT divert table, use the **show nat divert-table** command in privileged EXEC mode.

show nat divert-table [**self-addressed**] [**ipv6**] [**interface** *name*]

Syntax Description

ipv6	(Optional) Shows IPv6 entries in the divert table.
interface *name*	(Optional) Limits output to the specified source interface.
self-addressed	Show the self-addressed identity table.

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
8.4(2)	This command was added.
9.18(1)	The **self-addressed** keyword was added.

Usage Guidelines

Use the **show nat divert-table** command to show runtime representation of the NAT divert table. Use the **ipv6** optional keyword to view the IPv6 entries in the divert table. Use the interface optional keyword to view the NAT divert table for the specific source interface.

Starting with 9.18(1), you might see the following information in the output:

- **do-loopback=***interface* indicates that the divert rule will trigger loopback on the specified interface.
- **rst-possible-loopback=***interface* indicates that the divert rule is for from-the-box control plane (CP) traffic and loopback might or might not occur on the specified interface.
- **nlp-possible-loopback=***interface* indicates that the divert rule is for from/to-the-box non-Lina process (NLP) traffic and loopback might or might not occur on the specified interface.

Examples

The following is sample output from the **show nat divert-table** command:

```
ciscoasa# show nat divert-table
```

```
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

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

```
ciscoasa# show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

The following example shows the self-addressed table.

```
ciscoasa# show nat divert-table self-addressed

Self-Addressed Divert
192.168.1.33    255.255.255.255                         management to identity
1002::10        ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff    outside to identity
102.1.1.10      255.255.255.255                         outside to identity
1001::10        ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff    inside to identity
101.1.1.10      255.255.255.255                         inside to identity
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
show nat	Displays runtime representation of the NAT policies.

show nat pool

To display statistics of NAT pool usage, use the **show nat pool** command in privileged EXEC mode.

show nat pool [**interface** *if_name* [**ip** *address*] | **ip** *address*] [**detail**]
show nat pool cluster [**summary | interface** *if_name* [**ip** *address*] | **ip** *address*]

Syntax Description

cluster [**summary**]	(Optional) When ASA clustering is enabled, shows the current assignment of a PAT address to the owner unit and backup unit. (9.15+) Include the **summary** keyword to see the distribution of port blocks among the units in the cluster.
interface *if_name*	Limit the display to pools for the named interface. You can optionally include the **ip** keyword to futher limit the view.
ip *address*	Limit the display to the specified IP address from the PAT pool.
detail	Show information related to the usage and distribution of port blocks within a cluster. This keyword appears only if the unit is a cluster member. You cannot use it with the **cluster** keyword.

Command Default

This command has no default settings.

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
8.3(1)	This command was added.
8.4(3)	The output was modified to show the destination address for extended PAT. The PAT range was also modified depending on the use of the **flat** and **include-reserve** keywords.
9.0(1)	Support for IPv6 traffic and the **cluster** keyword to show the current assignment of a PAT address to the owner unit and backup unit were added.
9.15(1)	The following keywords were added: **interface** , **ip** , **detail** , **summary** .

Usage Guidelines

A NAT pool is created for each mapped protocol/IP address/port range. (Pre-9.15) The port ranges are 1-511, 512-1023, and 1024-65535 by default. If you use the **flat** keyword for a PAT pool in the **nat** command, you will see fewer, larger ranges.

(9.15+) Starting with 9.15, the port range is flat by default, and you can optionally include the reserved ports, 1-1023, in the pool. For clustered systems, the PAT pool is distributed among the cluster members in blocks of 512 ports.

Each NAT pool exists for at least 10 minutes after the last usage. The 10 minute hold-down timer is canceled if you clear the translations with **clear xlate** .

Examples

The following is sample output for the NAT pools created by a dynamic PAT rule shown by the **show running-config object network** command.

```
ciscoasa(config)# show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25
ciscoasa# show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

(Pre-9.15) The following is sample output from the **show nat pool** command showing use of the PAT pool **flat** option. Without the **include-reserve** keyword, two ranges are shown; the lower range is used when a source port below 1024 is mapped to the same port.

```
ciscoasa# show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

(Pre-9.15) The following is sample output from the **show nat pool** command showing use of the PAT pool **flat include-reserve** options.

```
ciscoasa# show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

(Pre-9.15) The following is sample output from the **show nat pool** command showing use of the PAT pool **extended flat include-reserve** options. The important items are the parenthetical addresses. These are the destination addresses used to extend PAT.

```
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
UDP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

(9.15+) The following example shows the distribution of port blocks (showing the port range), and their usage, in a cluster, including the unit that owns the block and the backup unit for the block.

```
ciscoasa# show nat pool cluster

IP outside_a:src_map_a 174.0.1.20
               [1536 – 2047], owner A, backup B
               [8192 – 8703], owner A, backup B
               [4089 – 4600], owner B, backup A
               [11243 – 11754], owner B, backup A
IP outside_a:src_map_a 174.0.1.21
               [1536 – 2047], owner A, backup B
               [8192 – 8703], owner A, backup B
               [4089 – 4600], owner B, backup A
               [11243 – 11754], owner B, backup A
IP outside_b:src_map_b 174.0.1.22
               [6656 - 7167], owner A, backup B
               [13312 - 13823], owner A, backup B
               [20480 - 20991], owner B, backup A
               [58368 - 58879], owner B, backup A
IP outside_b:src_map_b 174.0.1.23
               [46592 - 47103], owner A, backup B
               [52224 - 52735], owner A, backup B
               [62976 - 63487], owner B, backup A
```

(9.15+) The following example shows a summary of pool assignments in a cluster.

```
ciscoasa# show nat pool cluster summary

port-blocks count display order: total, unit-A, unit-B, unit-C, unit-D
IP outside_a:src_map_a, 174.0.1.20 (128 - 32/32/32/32)
IP outside_a:src_map_a, 174.0.1.21 (128 - 36/32/32/28)
IP outside_b:src_map_b, 174.0.1.22 (128 - 31/32/32/33)
```

(9.16+) The following example shows a summary of pool assignments in a cluster. Starting with 9.16, the information includes the number of reserved ports and reclaimed ports.

```
ciscoasa# show nat pool cluster summary

port-blocks count display order: total, unit-A, unit-B
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
IP Outside:Mapped-IPGroup 10.10.10.101 (126 - 63 / 63) ^ 0 # 0
```

(9.15+) The following example shows detailed PAT pool usage for the pools in a cluster.

```
ciscoasa# show nat pool detail

TCP PAT pool outside_a, address 174.0.1.1
                range 1536-2047, allocated 56
                range 8192-8703, allocated 16
UDP PAT pool outside_a, address 174.0.1.1
                range 1536-2047, allocated 12
                range 8192-8703, allocated 25
 TCP PAT pool outside_b, address 174.0.2.1
                range 47104-47615, allocated 39
                range 62464-62975, allocated 9
UDP PAT pool outside_b, address 174.0.2.1
                range 47104-47615, allocated 35
                range 62464-62975, allocated 27
```

(9.15+) The following example shows how to limit the view to a specific interface on a specific device.

```
ciscoasa# show nat pool interface outside_b ip 174.0.2.1

TCP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 0
TCP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 12
TCP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 48
UDP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 6
UDP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 8
UDP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 62
```

Related Commands

Command	Description
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
show nat	Displays NAT policy statistics.

show nat proxy-arp

To display the NAT proxy ARP table, use the **show nat proxy-arp** command in privileged EXEC mode.

show nat proxy-arp [**ipv6**] [**interface** *name*]

Syntax Description

ipv6	(Optional) Shows IPv6 entries in the proxy ARP table.
interface *name*	(Optional) Limits output to the specified source 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
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Use the **show nat proxy-arp** command to show runtime representation of the NAT proxy ARP table. Use the **ipv6** optional keyword to view the IPv6 entries in the proxy ARP table. Use the interface optional keyword to view the NAT proxy ARP table for the specific source interface.

Examples

The following is sample output from the **show nat proxy-arp** command:

```
ciscoasa# show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f5558bbbfc0, ip/id=10.10.1.134, mask=255.255.255.255 ifc=test2
 config:(inside) to (test2) source dynamic inside_v6 outside_v4_pat  destination
static inside_v6_nat any
id=0x00007f5558bbbfc0, ip/id=10.10.1.135, mask=255.255.255.255 ifc=test2
 config:(inside) to (test2) source dynamic inside_v6 outside_v4_pat  destination
static inside_v6_nat any
id=0x00007f55595ad2c0, ip/id=10.86.118.2, mask=255.255.255.255 ifc=inside
 config:(inside) to (test2) source dynamic inside_v6 interface  dns
id=0x00007f5559424e80, ip/id=10.100.10.1, mask=255.255.255.255 ifc=NP Identity Ifc
 config:(any) to (any) source dynamic src_network pat-pool mapped-pat-pool
id=0x00007f5559424e80, ip/id=10.100.10.2, mask=255.255.255.255 ifc=NP Identity Ifc
 config:(any) to (any) source dynamic src_network pat-pool mapped-pat-pool
id=0x00007f5544785700, ip/id=10.7.17.2, mask=255.255.255.254 ifc=NP Identity Ifc
```

```
 config:(any) to (any) source static test2 10.3.3.0
id=0x00007f554c4ae740, ip/id=10.1.1.1, mask=255.255.255.255 ifc=NP Identity Ifc
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
show nat	Displays runtime representation of the NAT policies.

show ntp associations

To view NTP association information, use the **show ntp associations** command in user EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Shows additional details about each association.

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
User EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ntp associations** command:

```
ciscoasa> show ntp associations
     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 10-2 shows each field description.

Table 2: show ntp associations Fields

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: • * —Synchronized to this peer. • # —Almost synchronized to this peer. • + —Peer selected for possible synchronization. • - —Peer is a candidate for selection. • ~ —Peer is statically configured, but not synchronized.
address	The address of the NTP peer.
ref clock	The address of the reference clock of the peer.
st	The stratum of the peer.
when	The time since the last NTP packet was received from the peer.
poll	The polling interval (in seconds).
reach	The peer reachability (as a bit string, in octal).
delay	The round-trip delay to the peer (in milliseconds).
offset	The relative time of the peer clock to the local clock (in milliseconds).
disp	The dispersion value.

Examples

The following is sample output from the **show ntp associations detail** command:

```
ciscoasa> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87   0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74   0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62   16000.0
```

Table 10-3 shows each field description.

Table 3: show ntp associations detail Fields

Field	Description
IP-address configured	The server (peer) IP address.
(status)	• our_master—The ASA is synchronized to this peer. • selected—Peer is selected for possible synchronization. • candidate—Peer is a candidate for selection.
(sanity)	• sane—The peer passes basic sanity checks. • insane—The peer fails basic sanity checks.
(validity)	• valid—The peer time is believed to be valid. • invalid—The peer time is believed to be invalid. • leap_add—The peer is signaling that a leap second will be added. • leap-sub—The peer is signaling that a leap second will be subtracted.
stratum	The stratum of the peer.
(reference peer)	unsynced—The peer is not synchronized to any other machine. ref ID—The address of the machine that the peer is synchronized to.
time	The last time stamp the peer received from its master.
our mode client	Our mode relative to the peer, which is always client.
peer mode server	The mode of the peer relative to the server.
our poll intvl	Our poll interval to the peer.
peer poll intvl	The peer poll interval to us.
root delay	The delay along the path to the root (ultimate stratum 1 time source).
root disp	The dispersion of the path to the root.
reach	The peer reachability (as a bit string in octal).
sync dist	The peer synchronization distance.
delay	The round-trip delay to the peer.
offset	The offset of the peer clock relative to our clock.
dispersion	The dispersion of the peer clock.
precision	The precision of the peer clock (in hertz).

Field	Description
version	The NTP version number that the peer is using.
org time	The originate time stamp.
rcv time	The receive time stamp.
xmt time	The transmit time stamp.
filtdelay	The round-trip delay (in milliseconds) of each sample.
filtoffset	The clock offset (in milliseconds) of each sample.
filterror	The approximate error of each sample.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show ntp status

To show the status of each NTP association, use the **show ntp status** command in user EXEC mode.

show ntp status

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
User EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ntp status** command:

```
ciscoasa> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

Table 10-4 shows each field description.

Table 4: show ntp status Fields

Field	Description
Clock	• synchronized—The ASA is synchronized to an NTP server. • unsynchronized—The ASA is not synchronized to an NTP server.
stratum	NTP stratum of this system.
reference	The address of the NTP server to which the ASA is synchronized.

Field	Description
nominal freq	The nominal frequency of the system hardware clock.
actual freq	The measured frequency of the system hardware clock.
precision	The precision of the clock of this system (in hertz).
reference time	The reference time stamp.
clock offset	The offset of the system clock to the synchronized peer.
root delay	The total delay along the path to the root clock.
root dispersion	The dispersion of the root path.
peer dispersion	The dispersion of the synchronized peer.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the ASA is associated.

show nve

To show the parameters, status and statistics of an NVE interface, use the **show nve** command in privileged EXEC mode.

show nve [**1**] [**summary**]

Syntax Description

1	(Optional) Specifies the NVE instance, which is always 1.
summary	(Optional) Only shows the status of the NVE interface, number of VNIs behind the NVE interface, and number of VTEPs discovered.

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
9.4(1)	We added this command.
9.17(1)	Added output for ASA Virtual cluster control link peer group. Added output for Geneve encapsulation.

Usage Guidelines

This command shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source-interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

Examples

See the following output for the **show nve 1** command:

```
ciscoasa(config)# show nve 1
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
```

```
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

See the following output for the **show nve 1** command for an ASA Virtual cluster:

```
ciscoasa(config)# show nve 1
nve 1, source-interface "vtep-ifc" is up (nve-only cluster is ON)
 IP address 10.0.0.1, subnet mask 255.255.255.0
 Encapsulation: vxlan
 Encapsulated traffic statistics:
   14310839 packets input, 2609747129 bytes
   14475972 packets output, 3145279720 bytes
   0 packets dropped
 Number of configured static peer VTEPs: 0
 Configured static peer group: cluster
    Configured static peer group VTEPs:
        IP address 10.0.0.4 MAC address 000c.295e.38ae (learned)
        IP address 10.0.0.3 MAC address 000c.2905.0050 (learned)
        IP address 10.0.0.2 MAC address 000c.2926.8a03 (learned)
 Number of discovered peer VTEPs: 3
    Discovered peer VTEPs:
        IP address 10.0.0.4
        IP address 10.0.0.3
        IP address 10.0.0.2
 Number of VNIs attached to nve 1: 1
 VNIs attached:
        vni 1: segment-id 1, mcast-group none
```

See the following output for the **show nve 1** command for an ASA Virtual Geneve interface:

```
ciscoasa# show nve 1
   nve 1, source-interface "outside" is up (nve-only cluster is OFF)
            IP address 10.0.1.11, subnet mask 255.255.255.0
            Encapsulation: geneve
            Encapsulated traffic statistics:
               1107 packets input, 84557 bytes
               83 packets output, 39784 bytes
               0 packets dropped
            Number of configured static peer VTEPs: 0
            Configured static peer group: N/A
            Number of discovered peer VTEPs: 0
            Number of VNIs attached to nve 1: 1
            VNIs attached:
               vni 1: segment-id none, aws-proxy on, mcast-group none
            NVE aws-proxy channel is on.
```

See the following output for the **show nve 1 summary** command:

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

show object

To display information about objects, including hit counts and IP addresses for network-service objects, use the **show object** command in privileged EXEC mode..

```
show object [count [detail] | forward-reference | hidden | id obj_name
| internal | network | network-service [obj_name [domain name] [detail
] | predefined | security | service ]]
```

Syntax Description

count [**detail**]	(Optional.) Shows a count for each type of object, and information on how many objects are used in various types of policy such as NAT. Include the **detail** keyword to see the hexadecimal object ID for each object instead of a general count of objects.
domain *domain_name*	(Optional.) For network-service objects specified by name, limit the information to a specific domain. For example, example.com.
Forward-reference	(Optional) Displays objects that are forward-referenced, that is, they are named but not yet defined.
Hidden	(Optional.) Displays objects that the system hides.
id *name*	(Optional) The name of the object you want to view. Capitalization matters. For example “object-name” does not match “Object-Name.”
Internal	(Optional.) Displays objects that are defined for internal system use.
Network	(Optional.) Displays network objects.
network-service [*obj_name* [**domain** *name*] [**detail**]	(Optional.) Show all network-service objects. Include the detail keyword to see the cached IP addresses associated with the object members. You can specify an object name limit the view to one object. Use the domain keyword to further limit the view to a given DNS domain name. You must also include the detail keyword to see system-defined network-service objects.
Security	(Optional.) Displays security group objects.
Service	(Optional.) Displays service objects.

Command Default

Without parameters, all user-defined and unhidden objects are shown.

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
9.17(1)	This command was introduced.

Example

The following example shows the object named partner-web. The hitcnt (hit count) number shows how often connections matched the object.

```
ciscoasa# show object id partner-web
object network-service "partner-web"
 subnet 10.100.10.0 255.255.255.0 tcp eq https (hitcnt=0)
```

The following example shows a count of the objects.

```
ciscoasa# show object count
object network-service "my-ns-1" (hitcnt=0)
 member of: "my-nsg-1"
 domain example.com (bid=133345) tcp eq www (hitcnt=0)

Total Object Summary
Object total count                          161
Object network                              6
Object service                              155
Object security                             0
Object network-service                      1
Object hidden                               5
Object predefined                           153
Object internal                             0
Object dummy                                0
Object NAT                                  1
Object VPN NAT                              0
Object Migration                            0
Object FQDN                                 0
```

The following example uses the detail keyword to show both user-defined and system-defined (dynamic) objects, which are used by AVC.

```
ciscoasa(config)# show object network-service detail
object network-service "my_app" (hitcnt = 917)
  description custom application
  domain X.com (bid=1082173639) ip (hitcnt=0)
object network-service "TikTok" dynamic (hitcnt = 917)
  description Video social networking application.
  app-id 4154
  domain abtest-va-tiktok.byteoversea.com (bid=1082173639) ip (hitcnt=0)
  domain bytedns.net (bid=1082306293) ip (hitcnt=0)
  domain byteicdn.com (bid=1082459677) ip (hitcnt=0)
```

```
  domain tiktok.com (bid=1090924371) ip (hitcnt=917)
object network-service "ADrive" dynamic (hitcnt = 0)
 description Online file storage and backup.
 app-id 17
 domain adrive.com (bid=82093933) ip (hitcnt=0)
object network-service "Amazon" dynamic (hitcnt = 12)
 description Online retailer of books and most other goods.
 app-id 24
 domain amazon.com (bid=82227107) ip (hitcnt=12)
 domain amazon.jobs (bid=82334771) ip (hitcnt=0)
```

Related Commands

Command	Description
avc	Enable Application Visibility and Control (AVC), downloads the Vulnerability Database (VDB), and creates the network-service objects and groups for the applications and categories.
clear object	Clears the object hit count.

show object-group

To display object group information and the relevant hit count if the object group is of the network or network-service object-group type, use the **show object-group** command in privileged EXEC mode.

show object-group [**count** [*options*] | **forward-reference** | **geolocation** | **id** *name* | **interface** | **network** | **security** | **service**]

show object-group network-service [*group_name* [**network-service-member** *member_name* [**domain** *domain_name*]] [**detail**]

Syntax Description

count	(Optional.) Show statistics related to the number of object groups and the number of objects in those groups, and how they are used. Without parameters, the output shows a count for each type of object, and information on how many objects are used in various types of policy such as NAT. You can add the following options to tailor the output: • **All**—Show counts and information about objects for all types. • **Child-group-object**—Shows counts and information about groups that are referenced within another object group. These objects are considered children of the containing group. • **Group-level**—Shows how many group levels are contained within the group. For example, if a group contains another group object, which itself contains groups, there are 3 levels. • **Internal**—Show counts and information about internal objects. • **Parent-object-group**—Shows counts and information about groups that include another object group. These objects are considered parents of the groups it contains. • **Redundant**—Show counts and information about redundant group objects, that is, objects that have the same contents. • **Unused**—Show counts and information about group objects defined in the configuration that are not used in any policy. • **Used**—Show counts and information about group objects that are used in policies.
detail	For network-service objects, show the cached IP addresses associated with the object members.You must also include the detail keyword to see system-defined network-service group objects.
domain *domain_name*	(Optional.) For network-service objects specified by name and member, limit the information to a specific domain for that member. For example, example.com.
forward-reference	(Optional.) Displays groups that are forward-referenced, that is, they are named but not yet defined.

geolocation	(Optional.) Displays geolocation objects groups.
id *object_group_name*	(Optional) Identifies an object group by name.
network	(Optional) Network-type objects.
network-service [*group_name*]	(Optional.) Network-service objects. You can specify the object name to limit the information to a single object.
network-service-member *member_name*	(Optional.) For network-service objects specified by name, limit the information to a specific member of that object.
security	(Optional) Security-type objects
service	(Optional) Service-type object.

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
8.3(1)	This command was added.
9.17(1)	We added the **network-service** keyword and its associated parameters.
9.18(1)	The **count** keyword was added.

Usage Guidelines

When you use the count keyword with a parameter, the display includes the following columns:

- Id—The object group Identifier
- OG type—The object-group type
- Grp Cnt—The number of items in this object group.
- Dyn cnt—The number of dynamic items in the object-group's count. For example, FQDN.
- V4 cnt—The number of IPv4 Addresses in the object group
- V6 cnt—The number of IPv6 Addresses in the object group
- ACL Cnt—The number of ACLs that use this object group
- NAT Cnt—The number of NAT rules that use this object group

- Parent OG—The number of groups that include this object. Count in this represent the parent object-group
- Child OG—The number of groups that this object includes.
- Grp Level—(Shown in group-level output only.) How many group levels are contained within the group. For example, if a group contains another group object, which itself contains groups, there are 3 levels.
- Object group Name—The name of the group object.

Examples

The following is sample output from the **show object-group** command and shows information about the network object group named “Anet”:

```
ciscoasa# show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

The following is sample output from the **show object-group** command and shows information about a service group:

```
ciscoasa (config)# show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
   object-group protocol C-grp-proto
   protocol-object ospf
```

The following is sample output from the **show object-group** command and shows information about a protocol:

```
ciscoasa (config)# show object-group protocol
object-group protocol C-grp-proto
   protocol-object ospf
```

The following example shows a network-service object and its hit counts. The various identifiers, such as network-service group ID (nsg-id), application ID (app-id), and bid are internal indexing numbers that you can ignore.

```
ciscoasa (config)# show object-group network-service FMC_NSG_4294969442
object-group network-service FMC_NSG_4294969442 (nsg-id 512/1)
 network-service-member "Facebook" dynamic
  description Facebook is a social networking service.
  app-id 629
  domain connect.facebook.net (bid=214491) ip (hitcnt=0)
  domain facebook.com (bid=370809) ip (hitcnt=0)
  domain fbcdn.net (bid=490321) ip (hitcnt=0)
  domain fbcdn-photos-a.akamaihd.net (bid=548791) ip (hitcnt=0)
  domain fbcdn-photos-e-a.akamaihd.net (bid=681143) ip (hitcnt=0)
  domain fbcdn-photos-b-a.akamaihd.net (bid=840741) ip (hitcnt=0)
  domain fbstatic-a.akamaihd.net (bid=1014669) ip (hitcnt=0)
  domain fbexternal-a.akamaihd.net (bid=1098051) ip (hitcnt=0)
  domain fbcdn-profile-a.akamaihd.net (bid=1217875) ip (hitcnt=0)
  domain fbcdn-creative-a.akamaihd.net (bid=1379985) ip (hitcnt=0)
  domain channel.facebook.com (bid=1524617) ip (hitcnt=0)
  domain fbcdn-dragon-a.akamaihd.net (bid=1683343) ip (hitcnt=0)
  domain contentcache-a.akamaihd.net (bid=1782703) ip (hitcnt=0)
  domain facebook.net (bid=1868733) ip (hitcnt=0)
```

```
 network-service-member "Google+ Videos" dynamic
  description Video sharing among Google+ community.
  app-id 2881
  domain plus.google.com (bid=2068293) ip (hitcnt=0)
 network-service-member "Instagram" dynamic
  description Mobile phone photo sharing.
  app-id 1233
  domain instagram.com (bid=2176667) ip (hitcnt=0)
 network-service-member "LinkedIn" dynamic
  description Career oriented social networking.
  app-id 713
  domain linkedin.com (bid=2317259) ip (hitcnt=0)
>
```

The following example shows object counts, so you have an idea of how many object groups there are, how many objects are contained in the groups, and how many are used in ACLs, NAT, and so forth. This information relates to the performance of the object group search feature.

```
ciscoasa(config)# show object-group count

Total Summary
Object-group count                          14
Object-group object count                   331
Object-group Dynamic count                  0
Object-group IPv4 count                     331
Object-group IPv6 count                     0
Object-group Used in ACL                    9
Object-group Used in NAT                    0
Object-group Unused                         5
Object-group Internal                       0
Object-group Dummy                          0
Redundant object-group in Network           4
Redundant object-group in IfC               0
```

The following example shows the hexadecimal ID (id=) for the objects when you have enabled object group search.

```
ciscoasa# show object-group
Object-group network SOG1 (id= 0xf0000004)
 network-object host 1.1.1.1
 network-object host 10.30.241.26
Object-group network SOG2 (id=0xf0000005)
 network-object host 1.1.1.1
Object-group network SOG3 (id= 0xf0000006)
 network-object host 1.1.1.1
```

The following example shows partial output that includes application category network-service groups created from the Vulnerability Database (VDB) when Application Visibility and Control (AVC) is enabled. You must include the **detail** keyword to see these system-defined dynamic objects. Without the **detail** keyword, you are shown user-defined objects only.

```
ciscoasa(config)# show object-group network-service detail
object-group network-service custom_app_blocking (id=0xfdff0000) (hitcnt=567)
 network-service-member "TikTok" dynamic (hitcnt = 567)
  domain abtest-va-tiktok.byteoversea.com (bid=1082173639) ip (hitcnt=0)
  domain bytedns.net (bid=1082306293) ip (hitcnt=0)
  domain tiktok.com (bid=1090924371) ip (hitcnt=917)
object-group network-service _news_ dynamic (id=0xfdff0041) (hitcnt=0)
 network-service-member "Toutiao" dynamic (hitcnt = 0)
  domain snssdk.com (bid=1947711413) ip (hitcnt=0)
  domain toutiaoapi.com (bid=1947766347) ip (hitcnt=0)
```

```
  domain toutiaoimg.com (bid=1947947451) ip (hitcnt=0)
  domain toutiao.com (bid=1948055257) ip (hitcnt=0)
  domain doh.zjurl.cn (bid=1948195377) ip (hitcnt=0)
```

The following example shows the network visibility group created for AVC. This network-service group includes all network-service objects created by AVC from the VDB. The name of the object is _avc_visibility_nsg_. You must also include the **detail** keyword.

```
ciscoasa# show object-group network-service _avc_visibility_nsg_ detail
object-group network-service _avc_visibility_nsg_ dynamic (id=0xfdff0000) (hitcnt=1391)
 network-service-member "ADrive" dynamic (hitcnt = 0)
  description Online file storage and backup.
  domain adrive.com (bid=149781) ip (hitcnt=0)
 network-service-member "Amazon" dynamic (hitcnt = 12)
  description Online retailer of books and most other goods.
  domain amazon.com (bid=353725) ip (hitcnt=12)
  domain amazon.jobs (bid=399283) ip (hitcnt=0)
  domain amazon.in (bid=557827) ip (hitcnt=0)
  domain amazon.es (bid=713345) ip (hitcnt=0)
  domain amazon.de (bid=893113) ip (hitcnt=0)
  domain amazon.co.uk (bid=1047807) ip (hitcnt=0)
  domain amazon.co.jp (bid=1068127) ip (hitcnt=0)
  domain amazon.ca (bid=1287853) ip (hitcnt=0)
  domain m.media-amazon.com (bid=1347445) ip (hitcnt=0)
```

The following example shows group level counts.

```
ciscoasa# show object-group count group-level
id          OG Type    Grp Cnt  Dyn Cnt  V4 CNT   V6 CNT   Parent OG  Child OG Grp Level
Object Group Name
0x80001beb  network    2        0        1        0        1          1        2
nest01
0x80001bec  network    1        0        1        0        1          1        3
nest0
0x80001bed  network    3        0        1        0        1          1        4
nest1
0x80001bee  network    1        0        1        0        1          1        5
nest2
0x80001bef  network    1        0        1        0        1          1        6
nest3
0x80001bf0  network    18       0        1        0        1          1        7
grp.local
0x80001bf1  network    1        0        1        0        1          1        8
nest5
0x80001bf2  network    1        0        1        0        1          1        9
nest6
0x80001bf3  network    1        0        1        0        1          0        10
nest7
0x80001bf5  network    1        0        0        0        1          0        2
nest9
```

The following example shows parent level counts.

```
ciscoasa# show object-group count parent-object-group
id          OG Type    Grp Cnt  Dyn Cnt  V4 CNT   V6 CNT   ACL CNT  NAT CNT  Parent OG
Child OG Object Group Name
0x8000003c  network    4        0        14       0        2        0        2          0
       DM_INLINE_NETWORK_2546
0x80000043  network    10       0        151      0        2        0        4          0
       DM_INLINE_NETWORK_7
0x8000004b  network    4        0        21       0        2        0        1          0
```

```
        DM_INLINE_NETWORK_39
```

The following example shows child level counts.

```
ciscoasa# show object-group count child-group-object
id          OG Type    Grp Cnt  Dyn Cnt  V4 CNT   V6 CNT   ACL CNT  NAT CNT  Parent OG
Child OG Object Group Name
0x8000003a  network    6        0        6        0        19       0        0          13
       SerZone2_Server
0x8000003b  network    6        0        6        0        22       0        0          12
       SerZone3_Server
0x8000003f  network    33       0        33       0        0        0        0          10
       Swift-HK-User
```

Related Commands

Command	Description
avc	Enable Application Visibility and Control (AVC), downloads the Vulnerability Database (VDB), and creates the network-service objects and groups for the applications and categories.
clear object-group	Clears the object group hit count.
show access list	Shows all access lists, relevant expanded access list entries, and hit counts.
show object	Shows objects and hit counts.

show ospf

To display the general information about the OSPF routing processes, use the **show ospf** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.

Command Default

Lists all OSPF processes if no *pid* is specified.

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)	Support for multiple context mode was added.

Usage Guidelines

If the *pid* is included, only information for the specified routing process is included.

Examples

The following is sample output from the **show ospf** command, showing how to display general information about a specific OSPF routing process:

```
ciscoasa# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

The following is sample output from the **show ospf** command, showing how to display general information about all OSPF routing processes:

```
ciscoasa# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf border-routers

To display the internal OSPF routing table entries to ABRs and ASBRs, use the **show ospf border-routers** command in privileged EXEC mode.

show ospf border-routers

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.
9.0(1)	Support for multiple context mode was added.

Examples

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

```
ciscoasa# show ospf border-routers
OSPF Process 109 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf database

To display the information contained in the OSPF topological database on the ASA, use the **show ospf database** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **database** [**router | network | summary | asbr-summary | external | nssa-external**] [*lsid*] [**internal**] [**self-originate | adv-router** *addr*]
show ospf [*pid* [*area_id*]] **database database-summary**

Syntax Description

addr	(Optional) Router address.
adv-router	(Optional) Advertised router.
area_id	(Optional) ID of the area that is associated with the OSPF address range.
asbr-summary	(Optional) Displays an ASBR list summary.
database	Displays the database information.
database-summary	(Optional) Displays the complete database summary list.
external	(Optional) Displays routes external to a specified autonomous system.
internal	(Optional) Routes that are internal to a specified autonomous system.
lsid	(Optional) LSA ID.
network	(Optional) Displays the OSPF database information about the network.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
pid	(Optional) ID of the OSPF process.
router	(Optional) Displays the router.
self-originate	(Optional) Displays the information for the specified autonomous system.
summary	(Optional) Displays a summary of the 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
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the ASA. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

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

```
ciscoasa# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)
                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3
                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC
                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

The following is sample output from the **show ospf database asbr-summary** command:

```
ciscoasa# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

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

```
ciscoasa# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
```

```
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

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

```
ciscoasa# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

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

```
ciscoasa# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

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

```
ciscoasa# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)
                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
```

```
Forward Address: 0.0.0.0
External Route Tag: 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf events

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

show 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	• Yes	—
User EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

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

```
ciscoasa# show ospf events
            OSPF Router with ID (192.168.77.1) (Process ID 5)
   1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
   2 Apr 27 16:33:23.556: Rescanning RIB:  0x00x0
   3 Apr 27 16:33:23.556: Service Redist scan:  0x00x0
```

Related Commands

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

show ospf flood-list

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

show ospf flood-list *interface_name*

Syntax Description

interface_name	The name of the interface for which to display neighbor 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the ASA. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

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

```
ciscoasa# show ospf flood-list outside
  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf interface

To display the OSPF-related interface information, use the **show ospf interface** command in privileged EXEC mode.

show ospf interface [*interface_name*]

Syntax Description

interface_name	(Optional) Name of the interface for which to display the OSPF-related 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When used without the *interface_name* argument, the OSPF information for all interfaces is shown.

Examples

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

```
ciscoasa# show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

show ospf neighbor

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

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

Syntax Description

detail	(Optional) Lists detail information for the specified router.
interface_name	(Optional) Name of the interface for which to display neighbor information.
nbr_router_id	(Optional) Router ID of the neighbor 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output from the **show ospf neighbor** command. It shows how to display the OSPF-neighbor information on a per-interface basis.

```
ciscoasa# show ospf neighbor outside
Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following is sample output from the **show ospf neighbor detail** command. It shows how to display the detailed information for the specified OSPF-neighbor.

```
ciscoasa# show ospf neighbor detail
Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
    Dead timer due in 0:00:24
    Neighbor is up for 01:42:15
    Index 5/5, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 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
neighbor	Configures OSPF routers interconnecting to non-broadcast networks.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf nsf

To display the OSPFv2 related NSF information, use the **show ospf nsf** command in privileged EXEC mode.

show ospf nsf

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 ospf nsf** command:

```
ciscoasa# show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
 Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
 OSPF restart state is
 Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
 Config wait timer interval 10, timer not running
 Dbase wait timer interval 120, timer not running
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF on NSF-capable router.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf request-list

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

show ospf request-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.
nbr_router_id	Router ID of the neighbor router. Displays the list of all LSAs that are requested by the router from this neighbor.

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.
9.0(1)	Support for multiple context mode was added.

Examples

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

```
ciscoasa# show ospf request-list 192.168.1.12 inside
          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12
  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

Command	Description
show ospf retransmission-list	Displays a list of all LSAs waiting to be resent.

show ospf retransmission-list

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

show ospf retransmission-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information.
nbr_router_id	Router ID of the neighbor 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the ASA. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

The *nbr_router_id* argument displays the list of all LSAs that are waiting to be resent for this neighbor.

The *interface_name* argument displays the list of all LSAs that are waiting to be resent for this interface.

Examples

The following is sample output from the **show ospf retransmission-list** command, where the *nbr_router_id* argument is 192.168.1.11 and the *if_name* argument is outside:

```
ciscoasa# show ospf retransmission-list 192.168.1.11 outside
          OSPF Router with ID (192.168.1.12) (Process ID 1)
  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

Command	Description
show ospf request-list	Displays a list of all LSAs that are requested by a router.

show ospf rib

To display the OSPF Router Information Base (RIB), use the **show ospf rib** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **rib** [*network_prefix* [*network_mask*] **| detail | redistribution** [*network_prefix* [*network_mask*] **| detail**]]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.
network_prefix [*network_mask*]	(Optional) The network prefix and optionally the mask of the route you want to view, for example: 10.100.10.1 10.100.10.0 255.255.255.0
detail	(Optional) Display detailed information about the RIB.
redistribution	(Optional) Display redistribution information. You can also specify the network prefix and mask or **detail** keyword after the redistribution keyword.

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)	Support for multiple context mode was added.

show ospf statistics

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

show ospf [*process_id*] **statistics** [**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	• Yes	—
User EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode 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 ospf statistics** command:

```
ciscoasa# show ospf 10 statistics 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 ospf	Shows all settings in the OSPF routing process.
show ospf border-routers	Shows the internal OSPF routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the **show ospf summary-address** command in privileged EXEC mode.

show ospf summary-address

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.
9.0(1)	MSupport for multiple context mode was added.

Examples

The following shows sample output from the **show ospf summary-address** command. It shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5.

```
ciscoasa# show ospf 5 summary-address
OSPF Process 2, Summary-address
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

Related Commands

Command	Description
summary-address	Creates aggregate addresses for OSPF.

show ospf traffic

To display a list of different types of packets that have been processed (sent or received) by a particular OSPF instance, use the **show ospf traffic** command in privileged EXEC mode. With this command, you can get a snapshot of the different types of OSPF packets that are being processed without enabling debugging. If there are two OSPF instances configured, the show ospf traffic command displays the statistics for both instances with the process ID of each instance. You can also display the statistics for a single instance by using the sho**w ospf** *process_id* **traffic** command.

show ospf 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
9.0(1)	This command was added.

Usage Guidelines

With this command, you can get a snapshot of the different types of OSPF packets that are being processed without enabling debugging. If there are two OSPF instances configured, the **show ospf traffic** command displays the statistics for both instances with the process ID of each instance. You can also display the statistics for a single instance by using the **show ospf** *process_id* **traffic** command.

Examples

The following shows sample output from the **show ospf traffic** command.

```
ciscoasa# show ospf traffic
OSPF statistics (Process ID 70):
       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

Related Commands

Command	Description
show ospf virtual-links	Displays the parameters and the current state of OSPF virtual links.

show ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the **show ospf virtual-links** command in privileged EXEC mode.

show 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	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

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

```
ciscoasa# show ospf virtual-links
Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.