CHAPTER 26

show debug through show ipv6 traffic Commands

show debug

To show the current debugging configuration, use the **show debug** command.

show debug [*command* [*keywords*]]

Syntax Description

command	(Optional) Specifies the debug command whose current configuration you want to view. For each *command*, the syntax following *command* is identical to the syntax supported by the associated **debug** command. For example, valid *keywords* following **show debug aaa** are the same as the valid keywords for the **debug aaa** command. Thus, **show debug aaa** supports an **accounting** keyword, which allows you to specify that you want to see the debugging configuration for that portion of AAA debugging.

Defaults

This command has no default settings.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The valid *command* values follow. For information about valid syntax after *command*, see the entry for **debug** *command*, as applicable.

Note The availability of each *command* value depends upon the command modes that support the applicable **debug** command.

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**

- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**

- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **xdmcp**

Examples

The following commands enable debugging for authentication, accounting, and Flash memory. The **show debug** command is used in three ways to demonstrate how you can use it to view all debugging configuration, debugging configuration for a specific feature, and even debugging configuration for a subset of a feature.

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

Related Commands

Command	Description
debug	See all **debug** commands.

show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command in privileged EXEC or global configuration mode.

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

Syntax Description

binding	Displays binding information for a given server IP address and its associated client hardware address and lease length.
IP_address	Shows the binding information for the specified IP address.
state	Displays the state of the DHCP server, such as whether it is enabled in the current context and whether it is enabled on each of the interfaces.
statistics	Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you include the optional IP address in the **show dhcpd binding** command, only the binding for that IP address is shown.

The **show dhcpd binding | state | statistics** commands are also available in global configuration mode.

Examples

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

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output from the **show dhcpd state** command:

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
```

```
Interface inside, Not Configured for DHCP
```

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

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
clear dhcpd	Clears the DHCP server bindings and statistic counters.
dhcpd lease	Defines the lease length for DHCP information granted to clients.
show running-config dhcpd	Displays the current DHCP server configuration.

show dhcprelay state

To view the state of the DHCP relay agent, use the **show dhcprelay state** command in privileged EXEC or global configuration mode.

show dhcprelay state

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command displays the DHCP relay agent state information for the current context and each interface.

Examples

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

```
hostname# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

Related Commands

Command	Description
show dhcpd	Displays DHCP server statistics and state information.
show dhcprelay statistics	Displays the DHCP relay statistics.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show dhcprelay statistics

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

show dhcprelay statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

Examples

The following shows sample output for the **show dhcprelay statistics** command:

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
FeralPix(config)#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay state	Displays the state of the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show disk

To display the contents of the Flash memory, use the **show disk** command in privileged EXEC mode. To view the Flash memory for a PIX security appliance, see the **show flash** command.

show disk[**0** | **1**] [**filesys** | **all**]

Syntax Description

**0	1**	Specifies the internal Flash memory (0, the default) or the external Flash memory (1).
filesys	Shows information about the compact Flash card.
all	Shows the contents of Flash memory plus the file system information,

Defaults

Shows the internal Flash memory by default.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

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

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
```

```
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

The following is sample output from the **show disk filesys** command:

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

Related Commands

Command	Description
dir	Displays the directory contents.
show flash	Displays the contents of the internal Flash memory.

show dns-hosts

To show the DNS cache, use the **show dns-hosts** command in privileged EXEC mode.The DNS cache includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the **name** command.

show dns-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

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		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show dns-hosts** command:

```
hostname# show dns-hosts
Host                      Flags      Age Type   Address(es)
ns2.example.com           (temp, OK) 0    IP    10.102.255.44
ns1.example.com           (temp, OK) 0    IP    192.168.241.185
snowmass.example.com      (temp, OK) 0    IP    10.94.146.101
server.example.com        (temp, OK) 0    IP    10.94.146.80
```

Table 26-1 shows each field description.

Table 26-1 show dns-hosts Fields

Field	Description
Host	Shows the hostname.
Flags	Shows the entry status, as a combination of the following: • temp—This entry is temporary because it comes from a DNS server. The security appliance removes this entry after 72 hours of inactivity. • perm—This entry is permanent because it was added with the **name** command. • OK—This entry is valid. • ??—This entry is suspect and needs to be revalidated. • EX—This entry is expired.
Age	Shows the number of hours since this entry was last referenced.
Type	Shows the type of DNS record; this value is always IP.
Address(es)	The IP addresses.

Related Commands

Command	Description
clear dns-hosts cache	Clears the DNS cache.
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.

show failover

To display information about the failover status of the unit, use the **show failover** command in privileged EXEC mode.

show failover [**group** *num* | **history** | **interface** | **state** | **statistics**]

Syntax Description

group	Displays the running state of the specified failover group.
history	Displays failover history. The failover history displays past failover state changes and the reason for the state change.
interface	Displays failover command and stateful link information.
num	Failover group number.
state	Displays the failover state of both failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and, if a unit is in the failed state, the reason for the failure.
statistics	Displays transmit and receive packet count of failover command interface.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified. The output includes additional information.

Usage Guidelines

The **show failover** command displays the dynamic failover information, interface status, and Stateful Failover statistics. The Stateful Failover Logical Update Statistics output appears only when Stateful Failover is enabled. The “xerr” and “rerr” values do not indicate errors in failover, but rather the number of packet transmit or receive errors.

In the **show failover** command output, the fields have the following values:

- Stateful Obj has these values:
  - xmit—Indicates the number of packets transmitted.
  - xerr—Indicates the number of transmit errors.
  - rcv—Indicates the number of packets received.
  - rerr—Indicates the number of receive errors.

- Each row is for a particular object static count as follows:
  - General—Indicates the sum of all stateful objects.
  - sys cmd—Refers to the logical update system commands, such as **login** or **stay alive**.
  - up time—Indicates the value for the security appliance up time, which the active security appliance passes on to the standby security appliance.
  - RPC services—Remote Procedure Call connection information.
  - TCP conn—Dynamic TCP connection information.
  - UDP conn—Dynamic UDP connection information.
  - ARP tbl—Dynamic ARP table information.
  - Xlate_Timeout—Indicates connection translation timeout information.
  - VPN IKE upd—IKE connection information.
  - VPN IPSEC upd—IPSec connection information.
  - VPN CTCP upd—cTCP tunnel connection information.
  - VPN SDI upd—SDI AAA connection information.
  - VPN DHCP upd—Tunneled DHCP connection information.

If you do not enter a failover IP address, the **show failover** command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remain in a "waiting" state. You must set a failover IP address for failover to work.

In multiple configuration mode, only the **show failover** command is available in a security context; you cannot enter the optional keywords.

Examples

The following is sample output from the **show failover** command for Active/Standby Failover. The security appliances are ASA 5500 series adaptive security appliances, each equipped with a CSC SSM as shown in the details for slot 1 of each security appliance.

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3): Normal
                  Interface outside (10.132.9.3): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4): Normal
                  Interface outside (10.132.9.4): Normal
```

```
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

The following is sample output from the **show failover** command for Active/Active Failover.

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)
```

```
                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

The following is sample output from the **show failover state** command for an active-active setup:

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

The following is sample output from the **show failover state** command for an active-standby setup:

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Table 26-2 describes the output of the **show failover state** command.

Table 26-2 show failover state Output Description

Field	Description
Configuration State	Displays the state of configuration synchronization. The following are possible configuration states for the standby unit: • **Config Syncing - STANDBY**—Set while the synchronized configuration is being executed. • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**—Set when the standby unit has completed a configuration synchronization from the active unit. The following are possible configuration states for the active unit: • **Config Syncing**—Set on the active unit when it is performing a configuration synchronization to the standby unit. • **Interface Config Syncing** • **Sync Done**—Set when the active unit has completed a successful configuration synchronization to the standby unit. • **Ready for Config Sync**—Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.
Communication State	Displays the status of the MAC address synchronization. • **Mac set**—The MAC addresses have been synchronized from the peer unit to this unit. • **Updated Mac**—Used when a MAC address is updated and needs to be synchronized to the other unit. Also used during the transition period where the unit is updating the local MAC addresses synchronized from the peer unit.
Date/Time	Displays a date and timestamp for the failure.
Last Failure Reason	Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information changes only when a failover occurs. The following are possible fail reasons: • **Ifc Failure**—The number of interfaces that failed met the failover criteria and caused failover. • **Comm Failure**—The failover link failed or peer is down. • **Backplane Failure**
State	Displays the Primary/Secondary and Active/Standby status for the unit.
This host/Other host	This host indicates information for the device upon which the command was executed. Other host indicates information for the other device in the failover pair.

Related Commands

Command	Description
show running-config failover	Displays the **failover** commands in the current configuration.

show file

To display information about the file system, use the **show file** command in privileged EXEC mode.

show file descriptors | system | information *filename*

Syntax Description

descriptors	Displays all open file descriptors.
information	Displays information about a specific file.
filename	Specifies the filename.
system	Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to display the file system information:

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

Related Commands

Command	Description
dir	Displays the directory contents.
pwd	Displays the current working directory.

show firewall

To show the current firewall mode (routed or transparent), use the **show firewall** command in privileged EXEC mode.

show firewall

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show firewall
Firewall mode: Router
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode.
show mode	Shows the current context mode, either single or multiple.

show flash

To display the contents of the internal Flash memory, use the **show flash:** command in privileged EXEC mode.

show flash:

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to display the contents of the internal Flash memory:

```
hostname# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log
```

```
10170368 bytes available (52711424 bytes used)
```

Related Commands

Command	Description
dir	Displays the directory contents.

show fragment

To display the operational data of the IP fragment reassembly module, enter the **show fragment** command in privileged EXEC mode.

show fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.

Defaults

If an *interface* is not specified, the command applies to all interfaces.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **show fragment** and **show running-config fragment**, to separate the configuration data from the operational data.

Examples

This example shows how to display the operational data of the IP fragment reassembly module:

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

A description of the fields used in the configuration example follows:

Assemble—The number of fragments that have been assembled.

Chain—The maximum number of allowed fragments in a single set.

Fail—The number of fragments that have not succeeded in being reassembled.

Overflow—The number of fragments that overflowed the queue.

Queue—The number of fragments waiting to be reassembled.

Size—The configured size of the database.

Timeout—The maximum number of seconds that we will hold on to the fragments, waiting to receive all of them, to perform the reassembly checks.

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show running-config fragment	Displays the IP fragment reassembly configuration.

show gc

To display the garbage collection process statistics, use the **show gc** command in privileged EXEC mode.

show gc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

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

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

Related Commands

Command	Description
clear gc	Removes the garbage collection process statistics.

show h225

To display information for H.225 sessions established across the security appliance, use the **show h225** command in privileged EXEC mode.

show h225

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show h225** command displays information for H.225 sessions established across the security appliance. Along with the **debug h323 h225 event**, **debug h323 h245 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Before using the **show h225**, **show h245**, or **show h323-ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** output to reach its end. If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

Examples

The following is sample output from the **show h225** command:

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
| Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
| 1. CRV 9861
| Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
| Local: | 10.130.56.4/1050 | Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the security appliance between the local endpoint 10.130.56.3 and foreign host 172.30.254.203, and for these particular endpoints, there is 1 concurrent call between them, with a CRV (Call Reference Value) for that call of 9861.

For the local endpoint 10.130.56.4 and foreign host 172.30.254.205, there are 0 concurrent Calls. This means that there is no active call between the endpoints even though the H.225 session still exists. This could happen if, at the time of the **show h225** command, the call has already ended but the H.225 session has not yet been deleted. Alternately, it could mean that the two endpoints still have a TCP connection opened between them because they set "maintainConnection" to TRUE, so the session is kept open until they set it to FALSE again, or until the session times out based on the H.225 timeout value in your configuration.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show h245

To display information for H.245 sessions established across the security appliance by endpoints using slow start, use the **show h245** command in privileged EXEC mode.

show h245

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the security appliance by endpoints using slow start. (Slow start is when the two endpoints of a call open another TCP control channel for H.245. Fast start is where the H.245 messages are exchanged as part of the H.225 messages on the H.225 control channel.) Along with the **debug h323 h245 event**, **debug h323 h225 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Examples

The following is sample output from the **show h245** command:

```
hostname# show h245
Total: 1
  | LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
  | MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
  | Local | 10.130.56.3 RTP 49608 RTCP 49609
  | MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
  | Local | 10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the security appliance. The local endpoint is 10.130.56.3, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0. (The TKTP header is a 4-byte header preceding each H.225/H.245 message. It gives

the length of the message, including the 4-byte header.) The foreign host endpoint is 172.30.254.203, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0.

The media negotiated between these endpoints have a LCN (logical channel number) of 258 with the foreign RTP IP address/port pair of 172.30.254.203/49608 and a RTCP IP address/port of 172.30.254.203/49609 with a local RTP IP address/port pair of 10.130.56.3/49608 and a RTCP port of 49609.

The second LCN of 259 has a foreign RTP IP address/port pair of 172.30.254.203/49606 and a RTCP IP address/port pair of 172.30.254.203/49607 with a local RTP IP address/port pair of 10.130.56.3/49606 and RTCP port of 49607.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show h323-ras

To display information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint, use the **show h323-ras** command in privileged EXEC mode.

show h323-ras

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show h323-ras** command displays information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint. Along with the **debug h323 ras event** and **show local-host** commands, this command is used for troubleshooting H.323 RAS inspection engine issues.

The **show h323-ras** command displays connection information for troubleshooting H.323 inspection engine issues, and is described in the **inspect protocol h323 {h225 | ras}** command page.

Examples

The following is sample output from the **show h323-ras** command:

```
hostname# show h323-ras
Total: 1
|GK|Caller
|172.30.254.214 10.130.56.14
hostname#
```

This output shows that there is one active registration between the gatekeeper 172.30.254.214 and its client 10.130.56.14.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show history

To display the previously entered commands, use the **show history** command in user EXEC mode.

show history

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show history** command lets you display previously entered commands. You can examine commands individually with the up and down arrows, enter **^p** to display previously entered lines, or enter **^n** to display the next line.

Examples

The following example shows how to display previously entered commands when you are in user EXEC mode:

```
hostname> show history
    show history
    help
    show history
```

The following example shows how to display previously entered commands in privileged EXEC mode:

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

This example shows how to display previously entered commands in global configuration mode:

```
hostname(config)# show history
    show history
    help
```

```
show history
enable
show history
config t
show history
```

Related Commands

Command	Description
help	Displays help information for the command specified.

show icmp

To display the ICMP configuration, use the **show icmp** command in privileged EXEC mode.

show icmp

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was previously existing.

Usage Guidelines

The **show icmp** command displays the ICMP configuration.

Examples

The following example shows the ICMP configuration:

```
hostname# show icmp
```

Related Commands

clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
inspect icmp	Enables or disables the ICMP inspection engine.
timeout icmp	Configures the idle timeout for ICMP.

show idb

To display information about the status of interface descriptor blocks, use the **show idb** command in privileged EXEC mode.

show idb

Syntax Description

This command has no arguments or keywords.

Defaults

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		
				Multiple	
	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

IDBs are the internal data structure representing interface resources. See the "Examples" section for a description of the display output.

Examples

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

```
hostname# show idb
Maximum number of Software IDBs 280.  In use 23.

                    HWIDBs     SWIDBs
             Active 6          21
           Inactive 1          2
         Total IDBs 7          23
 Size each (bytes) 116        212
        Total bytes 812        4876

HWIDB#   1 0xbb68ebc  Control0/0
HWIDB#   2 0xcd47d84  GigabitEthernet0/0
HWIDB#   3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#   4 0xcd5063c  GigabitEthernet0/2
HWIDB#   5 0xcd54a9c  GigabitEthernet0/3
HWIDB#   6 0xcd58f04  Management0/0

SWIDB#   1 0x0bb68f54 0x01010001 Control0/0
SWIDB#   2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#   3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
```

```
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

Table 26-1 shows each field description.

Table 26-3 show idb stats Fields

Field	Description
HWIDBs	Shows the statistics for all HWIDBs. HWIDBs are created for each hardware port in the system.
SWIDBs	Shows the statistics for all SWIDBs. SWIDBs are created for each main and subinterface in the system, and for each interface that is allocated to a context. Some other internal software modules also create IDBs.
HWIDB#	Specifies a hardware interface entry. The IDB sequence number, address, and interface name is displayed in each line.
SWIDB#	Specifies a software interface entry. The IDB sequence number, address, corresponding vPif id, and interface name are displayed in each line.
PEER IDB#	Specifies an interface allocated to a context. The IDB sequence number, address, corresponding vPif id, context id and interface name are displayed in each line.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show igmp groups

To display the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP, use the **show igmp groups** command in privileged EXEC mode.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	(Optional) Provides a detailed description of the sources.
group	(Optional) The address of an IGMP group. Including this optional argument limits the display to the specified group.
if_name	(Optional) Displays group information for the specified interface.
reserved	(Optional) Displays information about reserved groups.
summary	(Optional) Displays group joins summary information.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show igmp groups** command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples

The following is sample output from the **show igmp groups** command:

```
hostname#show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

show igmp interface

To display multicast information for an interface, use the **show igmp interface** command in privileged EXEC mode.

show igmp interface [*if_name*]

Syntax Description

if_name	(Optional) Displays IGMP group information for the selected interface.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was modified. The **detail** keyword was removed.

Usage Guidelines

If you omit the optional *if_name* argument, the **show igmp interface** command displays information about all interfaces.

Examples

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

```
hostname# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.

show igmp traffic

To display IGMP traffic statistics, use the **show igmp traffic** command in privileged EXEC mode.

show igmp traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                             Received     Sent
Valid IGMP Packets              3           6
Queries                         2           6
Reports                         1           0
Leaves                          0           0
Mtrace packets                  0           0
DVMRP packets                   0           0
PIM packets                     0           0

Errors:
Malformed Packets               0
Martian source                  0
Bad Checksums                   0
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP statistic counters.
clear igmp traffic	Clear the IGMP traffic counters.

show interface

To view interface statistics, use the **show interface** command in user EXEC mode.

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*] [**stats** | **detail**]

Syntax Description

detail	(Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled by the **asr-group** command. If you show all interfaces, then information about the internal interfaces for SSMs displays, if installed on the ASA 5500 series adaptive security appliance. The internal interface is not user-configurable, and the information is for debugging purposes only.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
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 **gigabitethernet0/1**. See the **interface** command for accepted values.
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not identify any options, this command shows basic statistics for all interfaces.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
User EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)(1)	This command was modified to include the new interface numbering scheme, and to add the **stats** keyword for clarity, and the **detail** keyword.
7.0(4)	This command added support for the 4GE SSM interfaces.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the security appliance shows only statistics for the current context. When you enter this command in the system execution space for a physical interface, the security appliance shows the combined statistics for all contexts.

The number of statistics shown for subinterfaces is a subset of the number of statistics shown for a physical interface.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context. If you set the **visible** keyword in the **allocate-interface** command, the security appliance shows the interface ID in the output of the **show interface** command.

See the "Examples" section for a description of the display output.

Examples

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

```
hostname> show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/7) software (0/0)
        output queue (curr/max blocks): hardware (0/13) software (0/0)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
```

```
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
```

Table 26-1 shows each field description.

Table 26-4 show interface Fields

Field	Description
Interface *ID*	The interface ID. Within a context, the security appliance shows the mapped name (if configured), unless you set the **allocate-interface** command **visible** keyword.
"*interface_name*"	The interface name set with the **nameif** command. In the system execution space, this field is blank because you cannot set the name in the system. If you do not configure a name, the following message appears after the Hardware line: `Available but not configured via nameif`
is *state*	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.

Table 26-4 show interface Fields (continued)

Field	Description
Line protocol is *state*	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.
VLAN identifier	For subinterfaces, the VLAN ID.
Hardware	The interface type, maximum bandwidth, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses. The following list describes the common hardware types: • i82542 - Intel PCI Fiber Gigabit card used on PIX platforms • i82543 - Intel PCI-X Fiber Gigabit card used on PIX platforms • i82546GB - Intel PCI-X Copper Gigabit used on ASA platforms • i82547GI - Intel CSA Copper Gigabit used as backplane on ASA platforms • i82557 - Intel PCI Copper Fast Ethernet used on ASA platforms • i82559 - Intel PCI Copper Fast Ethernet used on PIX platforms VCS7380 - Vitesse Four Port Gigabit Switch used in SSM-4GE
Media-type	(For 4GE SSM interfaces only) Shows if the interface is set as RJ-45 or SFP.

message area	A message might be displayed in some circumstances. See the following examples:
	• In the system execution space, you might see the following message:
	`Available for allocation to a context`
	• If you do not configure a name, you see the following message:
	`Available but not configured via nameif`

MAC address	The interface MAC address.
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows “MTU not set.”
IP address	The interface IP address set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows “IP address unassigned” because you cannot set the IP address in the system.
Subnet mask	The subnet mask for the IP address.
Packets input	The number of packets received on this interface.
Bytes	The number of bytes received on this interface.
No buffer	The number of received packets discarded because there was no buffer space in the main system. Compare this with the ignored count. Broadcast storms on Ethernet networks are often responsible for no input buffer events.
Received:	
Broadcasts	The number of broadcasts received.

Table 26-4 show interface Fields (continued)

Field	Description
Runts	The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants	The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Input errors	The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
CRC	The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the security appliance notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	The number of times that the security appliance was incapable of handing received data to a hardware buffer because the input rate exceeded the security appliance capability to handle the data.
Ignored	The number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
Abort	This field is not used. The value is always 0.
L2 decode drops	The number of packets dropped because the name is not configured (**nameif** command) or a frame with an invalid VLAN id is received.
Packets output	The number of packets sent on this interface.
Bytes	The number of bytes sent on this interface.
Underruns	The number of times that the transmitter ran faster than the security appliance could handle.
Output Errors	The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
Collisions	The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.

Table 26-4 show interface Fields (continued)

Field	Description
Interface resets	The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the security appliance resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
Babbles	Unused. ("babble" means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)
Late collisions	The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the security appliance is partly finished sending the packet. The security appliance does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.
Deferred	The number of frames that were deferred before transmission due to activity on the link.
Rate limit drops	(For 4GE SSM interfaces only) The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps.
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.
Input queue (curr/max blocks):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
Output queue (curr/max blocks):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
Traffic Statistics:	The number of packets received, transmitted, or dropped.
Packets input	The number of packets received and the number of bytes.
Packets output	The number of packets transmitted and the number of bytes.
Packets dropped	The number of packets dropped.

The following is sample output from the **show interface detail** command. The following example shows detailed interface statistics for all interfaces, including the internal interfaces (if present for your platform) and asymmetrical routing statistics, if enabled by the **asr-group** command:

```
hostname> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/7) software (0/0)
        output queue (curr/max blocks): hardware (0/13) software (0/0)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/2) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

Table 26-5 shows each field description for the **show interface detail** command. See Table 26-1 for fields that are also shown for the **show interface** command.

Table 26-5 show interface detail Fields

Field	Description
Demux drops	(On Internal-Data interface only) The number of packets dropped because the security appliance was unable to demultiplex packets from SSM interfaces. SSM interfaces communicate with the native interfaces across the backplane, and packets from all SSM interfaces are multiplexed on the backplane.
Control Point Interface States:	
Interface number	A number used for debugging that indicates in what order this interface was created, starting with 0.

Table 26-5 show interface detail Fields (continued)

Field	Description
Interface config status	The administrative state, as follows: • active—The interface is not shut down. • not active—The interface is shut down with the **shutdown** command.
Interface state	The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the security appliance brings the interfaces up or down as needed.
Asymmetrical Routing Statistics:	
Received X1 packets	Number of ASR packets received on this interface.
Transmitted X2 packets	Number of ASR packets sent on this interfaces.
Dropped X3 packets	Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
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 interface ip brief

To view interface IP addresses and status, use the **show interface ip brief** command in privileged EXEC mode.

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*] **ip brief**

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
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 **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance shows all interfaces.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip brief** command:

```
hostname# show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

Table 26-5 shows each field description.

Table 26-6 show interface ip brief Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command. If you show all interfaces, then information about the internal interface for the AIP SSM displays, if installed on the ASA adaptive security appliance. The internal interface is not user-configurable, and the information is for debugging purposes only.
IP-Address	The interface IP address.
OK?	This column is not currently used, and always shows "Yes."
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.
Status	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.
Protocol	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show inventory

To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the **show inventory** command in user EXEC or privileged EXEC mode. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

show inventory [**slot**]

Syntax Description

slot	(Optional) Specifies the SSM slot number (the system is slot 0)

Defaults

If you do not specify a slot to show inventory for:

- Show inventory information of all SSMs (including for power supply)

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Minor semantic changes.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Examples

The following is sample output from the **show inventory** command without any keywords or arguments. This sample output displays a list of Cisco entities installed in a router that are assigned a PID.

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC   , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999
```

Table 26-7describes the fields shown in the display.

Table 26-7 show inventory Field Descriptions

Field	Description
Name	Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

Related Commands

Command	Description
show diag	Displays diagnostic information about the controller, interface processor, and port adapters for a networking device.
show tech-support	Displays general information about the router when it reports a problem.

show ip address

To view interface IP addresses or, for transparent mode, the management IP address, use the **show ip address** command in privileged EXEC mode.

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
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 **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance shows all interface IP addresses.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command shows the primary IP addresses (called "System" in the display) for when you configure high availability as well as the current IP addresses. If the unit is active, then the system and current IP addresses match. If the unit is standby, then the current IP addresses show the standby addresses.

Examples

The following is sample output from the **show ip address** command:

```
hostname# show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
```

```
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
```

Table 26-5 shows each field description.

Table 26-8 show ip address Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command.
Name	The interface name set with the **nameif** command.
IP address	The interface IP address.
Subnet mask	The IP address subnet mask.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.

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	Displays the runtime status and statistics of interfaces.
show interface ip brief	Shows the interface IP address and status.

show ip address dhcp

To view detailed information about the DHCP lease or server for an interface, use the **show ip address dhcp** command in privileged EXEC mode.

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
lease	Shows information about the DHCP lease.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
server	Shows information about the DHCP server.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed to include the **lease** and **server** keywords to accommodate the new server functionality.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip address dhcp lease** command:

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
```

```
Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
Next timer fires after:111797 secs
Retry count:0, Client-ID:cisco-0000.0000.0000-outside
Proxy: TRUE  Proxy Network: 10.1.1.1
Hostname: device1
```

Table 26-5 shows each field description.

Table 26-9 show ip address dhcp lease Fields

Field	Description
Temp IP Addr	The IP address assigned to the interface.
Temp sub net mask	The subnet mask assigned to the interface.
DHCP Lease server	The DHCP server address.
state	The state of the DHCP lease, as follows: • Initial—The initialization state, where the security appliance begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails. • Selecting—The security appliance is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one. • Requesting—The security appliance is waiting to hear back from the server to which it sent its request. • Purging—The security appliance is removing the lease because of the client has released the IP address or there was some other error. • Bound—The security appliance has a valid lease and is operating normally. • Renewing—The security appliance is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply. • Rebinding—The security appliance failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends. • Holddown—The security appliance started the process to remove the lease. • Releasing—The security appliance sends release messages to the server indicating that the IP address is no longer needed.
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.
Lease	The length of time, specified by the DHCP server, that the interface can use this IP address.
Renewal	The length of time until the interface automatically attempts to renew this lease.

Table 26-9 show ip address dhcp lease Fields (continued)

Field	Description
Rebind	The length of time until the security appliance attempts to rebind to a DHCP server. Rebinding occurs if the security appliance cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The security appliance then attempts to contact any available DHCP server by broadcasting DHCP requests.
Temp default-gateway addr	The default gateway address supplied by the DHCP server.
Temp ip static route0	The default static route.
Next timer fires after	The number of seconds until the internal timer triggers.
Retry count	If the security appliance is attempting to establish a lease, this field shows the number of times the security appliance tried sending a DHCP message. For example, if the security appliance is in the Selecting state, this value shows the number of times the security appliance sent discover messages. If the security appliance is in the Requesting state, this value shows the number of times the security appliance sent request messages.
Client-ID	The client ID used in all communication with the server.
Proxy	Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
Proxy Network	The requested network.
Hostname	The client hostname.

The following is sample output from the **show ip address dhcp server** command:

```
hostname# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

Table 26-10 shows each field description.

Table 26-10 show ip address dhcp server Fields

Field	Description
DHCP server	The DHCP server address from which this interface obtained a lease. The top entry (“ANY”) is the default server and is always present.
Leases	The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.

Table 26-10 show ip address dhcp server Fields (continued)

Field	Description
Offers	The number of offers from the server.
Requests	The number of requests sent to the server.
Acks	The number of acknowledgements received from the server.
Naks	The number of negative acknowledgements received from the server.
Declines	The number of declines received from the server.
Releases	The number of releases sent to the server.
Bad	The number of bad packets received from the server.
DNS0	The primary DNS server address obtained from the DHCP server.
DNS1	The secondary DNS server address obtained from the DHCP server.
WINS0	The primary WINS server address obtained from the DHCP server.
WINS1	The secondary WINS server address obtained from the DHCP server.
Subnet	The subnet address obtained from the DHCP server.
DNS Domain	The domain obtained from the DHCP server.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip audit count

To show the number of signature matches when you apply an audit policy to an interface, use the **show ip audit count** command in privileged EXEC mode.

show ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Shows the number of matches for all interfaces.
interface *interface_name*	(Optional) Shows the number of matches for the specified interface.

Defaults

If you do not specify a keyword, this command shows the matches for all interfaces (**global**).

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To create an audit policy, use the **ip audit name** command, and to apply the policy, use the **ip audit interface** command.

Examples

The following is sample output from the **show ip audit count** command:

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

Related Commands

Command	Description
clear ip audit count	Clears the count of signature matches for an audit policy.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

show ip verify statistics

To show the number of packets dropped because of the Unicast RPF feature, use the **show ip verify statistics** command in privileged EXEC mode. Use the **ip verify reverse-path** command to enable Unicast RPF.

show ip verify statistics [interface *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows statistics for the specified interface.

Defaults

This command shows statistics for all interfaces.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ip verify statistics** command:

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

show ipsec sa

To display a list of IPSec SAs, use the **show ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec sa**.

show ipsec sa [**entry | identity | map** *map-name* **| peer** *peer-addr*] [**detail**]

Syntax Description

detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPSec SAs sorted by peer address
identity	(Optional) Displays IPSec SAs for sorted by identity, not including ESPs. This is a condensed form.
map *map-name*	(Optional) Displays IPSec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPSec SAs for specified peer IP addresses.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, displays IPSec SAs.

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
```

```
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

The following example, entered in global configuration mode, displays IPSec SAs for a crypto map named def.

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
```

```
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs for the keyword **entry**.

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
```

```
          sa timing: remaining key lifetime (sec): 429
          IV size: 8 bytes
          replay detection support: Y
      outbound esp sas:
        spi: 0xDC15BF68 (3692412776)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 429
          IV size: 8 bytes
          replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 212
          IV size: 8 bytes
          replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 212
          IV size: 8 bytes
          replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs with the keywords **entry detail**.

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example shows IPSec SAs with the keyword **identity**.

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPSec SAs with the keywords **identity** and **detail**.

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
```

```
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68

  Crypto map tag: def, local addr: 172.20.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0

    #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
    #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show ipsec sa summary

To display a summary of IPSec SAs, use the **show ipsec sa summary** command in global configuration mode or privileged EXEC mode.

show ipsec sa summary

Syntax Description

This command has no arguments or variables.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, displays a summary of IPSec SAs by the following connection types:

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN load balancing

```
hostname(config)# show ipsec sa summary

Current IPSec SA's:           Peak IPSec SA's:
IPSec            :     2        Peak Concurrent SA  :    14
IPSec over UDP   :     2        Peak Concurrent L2L :     0
IPSec over NAT-T :     4        Peak Concurrent RA  :    14
IPSec over TCP   :     6
IPSec VPN LB     :     0
Total            :    14
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Removes IPSec SAs entirely or based on specific parameters.
show ipsec sa	Displays a list of IPSec SAs.
show ipsec stats	Displays a list of IPSec statistics.

show ipsec stats

To display a list of IPSec statistics, use the **show ipsec stats** command in global configuration mode or privileged EXEC mode.

show ipsec stats

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, displays IPSec statistics:

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
```

```
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Clears IPSec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPSec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPSec SAs.

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 security appliance.

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.

Defaults

Displays all IPv6 access lists.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname# 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 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.

Defaults

Displays all IPv6 interfaces.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

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*.

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:

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  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:

```
hostname# 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
```

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.

```
hostname# 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 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 configure by the **nameif** command, only.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

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**—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**
  Interface from which the address was reachable.

Examples

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

```
hostname# 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:

```
hostname# 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 route

To display the contents of the IPv6 routing table, use the **show ipv6 route** command in privileged EXEC mode.

show ipv6 route

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

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.

Examples

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

```
hostname# 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
```

Related Commands

Command	Description
debug ipv6 route	Displays debug 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.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

```
hostname# 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.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

```
hostname# 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.