

serverfarm

To associate a real server farm with a virtual server, use the **serverfarm** command in SLB virtual server configuration mode. To remove the server farm association from the virtual server configuration, use the **no** form of this command.

serverfarm *serverfarm-name*

no serverfarm

Syntax Description	<i>serverfarm-name</i>	Name of a server farm that has already been defined using the ip slb serverfarm command.
---------------------------	------------------------	---

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	SLB virtual server configuration
----------------------	----------------------------------

Command History	Release	Modification
	12.0(7)XE	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples The following example shows how the **ip slb vserver**, **virtual**, and **serverfarm** commands are used to associate the real server farm named PUBLIC with the virtual server named PUBLIC_HTTP:

```
ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
serverfarm PUBLIC
```

Related Commands	Command	Description
	show ip slb vservers	Displays information about the virtual servers.
	virtual	Configures the virtual server attributes.

service dhcp

To enable the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent features on your router, use the **service dhcp** command in global configuration mode. To disable the Cisco IOS DHCP server and relay agent features, use the **no** form of this command.

service dhcp

no service dhcp

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The BOOTP and DHCP servers in Cisco IOS software both use the ICMP port (port 67) by default. ICMP “port unreachable messages” will only be returned to the sender if both the BOOTP server and DHCP server are disabled. Disabling only one of the servers will not result in ICMP port unreachable messages.

Examples

The following example enables DHCP services on the DHCP server:

```
service dhcp
```

show access-lists

To display the contents of current access lists, use the **show access-lists** command in privileged EXEC mode.

show access-lists [*access-list-number* | *access-list-name*]

Syntax Description		
<i>access-list-number</i>	(Optional) Number of the access list to display. The system displays all access lists by default.	
<i>access-list-name</i>	(Optional) Name of the IP access list to display.	

Defaults The system displays all access lists.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(5)T	The command output was modified to identify compiled access lists.
	12.2(2)T	The command output was modified to show information for IPv6 access lists.

Examples The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101

Extended IP access list 101
  permit tcp host 198.92.32.130 any established (4304 matches) check=5
  permit udp host 198.92.32.130 any eq domain (129 matches)
  permit icmp host 198.92.32.130 any
  permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
  permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
  permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
  permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
  permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
  permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
  deny ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
  deny ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
  deny ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
  deny ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
  deny ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the **show access-lists** command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

**Note**

The permit and deny information displayed by the **show access-lists** command may not be in the same order as that entered using the **access-list** command

```
Router# show access-lists

Standard IP access list 1 (Compiled)
  deny any
Standard IP access list 2 (Compiled)
  deny 192.168.0.0, wildcard bits 0.0.0.255
  permit any
Standard IP access list 3 (Compiled)
  deny 0.0.0.0
  deny 192.168.0.1, wildcard bits 0.0.0.255
  permit any
Standard IP access list 4 (Compiled)
  permit 0.0.0.0
  permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists

IPv6 access list list2
  deny ipv6 FEC0:0:0:2::/64 any sequence 10
  permit ipv6 any any sequence 20
```

For information on how to configure access lists, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*.

For information on how to configure dynamic access lists, refer to the “Traffic Filtering and Firewalls” part of the *Cisco IOS Security Configuration Guide*.

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

show access-list compiled

To display a table showing Turbo Access Control Lists (ACLs), use the **show access-list compiled** command in EXEC mode.

show access-list compiled

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command is used to display the status and condition of the Turbo ACL tables associated with each access list. The memory usage is displayed for each table; large and complex access lists may require substantial amounts of memory. If the memory usage is greater than the memory available, you can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the access lists is not then enabled.

Examples

The following is partial sample output from the **show access-list compiled** command:

```
Router# show access-list compiled

Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
  ACL          State      Tables  Entries  Config  Fragment  Redundant  Memory
1           Operational  1        2         1         0         0         1Kb
2           Operational  1        3         2         0         0         1Kb
3           Operational  1        4         3         0         0         1Kb
4           Operational  1        3         2         0         0         1Kb
5           Operational  1        5         4         0         0         1Kb
9           Operational  1        3         2         0         0         1Kb
20          Operational  1        9         8         0         0         1Kb
21          Operational  1        5         4         0         0         1Kb
101         Operational  1       15         9         7         2         1Kb
102         Operational  1       13         6         6         0         1Kb
120         Operational  1        2         1         0         0         1Kb
199         Operational  1        4         3         0         0         1Kb
First level lookup tables:
Block      Use              Rows      Columns  Memory used
0      TOS/Protocol      6/16     12/16    66048
1      IP Source (MS)   10/16    12/16    66048
2      IP Source (LS)   27/32    12/16   132096
```

■ show access-list compiled

3	IP Dest (MS)	3/16	12/16	66048
4	IP Dest (LS)	9/16	12/16	66048
5	TCP/UDP Src Port	1/16	12/16	66048
6	TCP/UDP Dest Port	3/16	12/16	66048
7	TCP Flags/Fragment	3/16	12/16	66048

Related Commands

Command	Description
access-list compiled	Enables the Turbo ACL feature.
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Creates a standard access list.
clear access-list counters	Clears the counters of an access list.
clear access-temp	Manually clears a temporary access list entry from a dynamic access list.
ip access-list	Defines an IP access list by name.
show ip access-list	Displays the contents of all current IP access lists.

show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** privileged EXEC command.

show arp

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following is sample output from the **show arp** command:

Router# **show arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	131.108.42.112	120	0000.a710.4baf	ARPA	Ethernet3
AppleTalk	4028.5	29	0000.0c01.0e56	SNAP	Ethernet2
Internet	131.108.42.114	105	0000.a710.859b	ARPA	Ethernet3
AppleTalk	4028.9	-	0000.0c02.a03c	SNAP	Ethernet2
Internet	131.108.42.121	42	0000.a710.68cd	ARPA	Ethernet3
Internet	131.108.36.9	-	0000.3080.6fd4	SNAP	TokenRing0
AppleTalk	4036.9	-	0000.3080.6fd4	SNAP	TokenRing0
Internet	131.108.33.9	-	0000.0c01.7bbd	SNAP	Fddi0

[Table 2](#) describes the significant fields shown in the display.

Table 2 *show arp Field Descriptions*

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

Table 2 *show arp Field Descriptions (continued)*

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: <ul style="list-style-type: none">• ARPA• SNAP• ETLK (EtherTalk)• SMDS
Interface	Indicates the interface associated with this network address.

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

```
show glbp [interface-type interface-number] [group] [state] [brief]
```

Syntax Description	
<i>interface-type</i>	(Optional) Interface type and number for which output is displayed.
<i>interface-number</i>	
<i>group</i>	(Optional) GLBP group number in the range from 0 to 1023.
<i>state</i>	(Optional) State of the GLBP router, one of the following: active , disabled , init , listen , speak , or standby .
brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(14)S	This command was introduced.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines Use the **show glbp** command to display information about GLBP groups on a router. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder.

Examples The following is sample output from the **show glbp** command:

```
Router# show glbp

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication text "stringabc"
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
```

show glbp

```
Owner ID is 0005.0050.6c08
Redirection enabled
Preemption enabled, min delay 60 sec
Active is local, weighting 105
```

The following is sample output from the **show glbp** command with the **brief** keyword specified:

```
Router# show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Fa0/0	10	-	254	Active	10.21.8.10	local	unknown
Fa0/0	10	1	7	Active	0007.b400.0101	local	-

[Table 3](#) describes the significant fields shown in the displays.

Table 3 *show glbp Field Descriptions*

Field	Description
FastEthernet0/0 - Group	Interface type and number and GLBP group number for the interface.
State is	<p>State descriptions for virtual gateways or virtual forwarders are similar but differ in some details. For a virtual gateway the state can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Indicates that the virtual IP address has not been configured or learned yet, but other GLBP configuration exists. • Initial—The virtual IP address has been configured or learned but virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen—Virtual gateway is receiving hello packets and is ready to change to the “speak” state if the active or standby virtual gateway becomes unavailable. • Speak—Virtual gateway is attempting to become the active or standby virtual gateway. • Standby—Indicates that the gateway is next in line to be the active virtual gateway (AVG). • Active—Indicates that this gateway is the AVG, and that it is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. <p>For a virtual forwarder the state can be one of the following:</p> <ul style="list-style-type: none"> • Disabled—Indicates that the virtual MAC address has not been assigned or learned. This is a transitory state because a virtual forwarder changing to a disabled state is deleted. • Initial—The virtual MAC address is known but virtual forwarder configuration is not complete. An interface must be up and configured to route IP, an interface IP address must be configured, and the virtual IP address must be known. • Listen—Virtual forwarder is receiving hello packets and is ready to change to the “active” state if the active virtual forwarder (AVF) becomes unavailable. • Active—Indicates that this gateway is the AVF, and that it is responsible for forwarding packets sent to the virtual forwarder MAC address.
Virtual IP address is	The virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the router has failed to defend its ARP cache entry.

Table 3 *show glbp Field Descriptions (continued)*

Field	Description
Hello time, hold time	The hello time is the time between hello packets (in seconds or milliseconds). The holdtime is the time (in seconds) before other routers declare the active router to be down. All routers in a GLBP group use the hello and holdtime values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello time and holdtime values.
Next hello sent in	Time until GLBP will send the next hello packet (in seconds or milliseconds).
Preemption enabled	Indicates whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time (in seconds) a higher-priority nonactive router will wait before preempting the lower-priority active router. This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.
Active is	Value can be "local," "unknown," or an IP address. Address (and the expiration date of the address) of the current AVG. This field is also displayed under the forwarder section where it indicates the address of the current AVF.
Standby is	Value can be "local," "unknown," or an IP address. Address (and the expiration date of the address) of the standby gateway (the gateway that is next in line to be the AVG).
Weighting	Initial weighting value with lower and upper threshold values.
Track object	List of objects that are being tracked and their corresponding states.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other routers declare the active GLBP router to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses, use the **show hosts** command in EXEC mode.

show hosts

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	This command was updated to support the Cisco modem user interface feature.

Examples

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

```
Router# show hosts
```

```
Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host          Flag      Age    Type    Address(es)
SLAG.CISCO.COM (temp, OK) 1      IP      172.20.4.10
CHAR.CISCO.COM (temp, OK) 8      IP      192.168.7.50
CHAOS.CISCO.COM (temp, OK) 8      IP      172.20.1.115
DIRT.CISCO.COM (temp, EX) 8      IP      172.20.1.111
DUSTBIN.CISCO.COM (temp, EX) 0      IP      172.20.1.27
DREGS.CISCO.COM (temp, EX) 24     IP      172.20.1.30
```

[Table 4](#) describes the significant fields shown in the display.

Table 4 *show hosts* Field Descriptions

Field	Description
Flag	A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. A permanent entry is entered by a configuration command and is not timed out. Entries marked OK are believed to be valid. Entries marked ?? are considered suspect and subject to revalidation. Entries marked EX are expired.
Age	Indicates the number of hours since the software last referred to the cache entry.
Type	Identifies the type of address, for example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the ip hp-host global configuration command, the show hosts command will display these host names as type HP-IP.
Address(es)	Displays the address of the host. One host may have up to eight addresses.

The following is sample output from a router when a modem telephone number is mapped to an IP host address for the Cisco modem user interface feature using the **ip host** global configuration command:

```
Router# show hosts

Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Codes: u - unknown, e - expired, * - OK, ? - revalidate
        t - temporary, p - permanent

      Host                Age  Type    Address(es)
*p p4085554567           0   IP      1.2.1.6
*p t4085551234           0   IP      1.2.1.5
```

Under the Host field, a “p” preceding the number indicates a pulse-dialed modem telephone number, and a “t” indicates a tone-dialed modem telephone number. The IP address mapped to the telephone number appears under the Address(es) field. See [Table 4](#) for descriptions of the other fields seen in this display.

Related Commands

Command	Description
clear arp interface	Deletes entries from the host name-to-address cache.
ip helper-address	Defines a static host-name-to-address mapping in the host cache.

show interface mac

To display MAC accounting information for interfaces configured for MAC accounting, use the **show interface mac** command in user EXEC or privileged EXEC mode.

show interface [*type number*] **mac**

Syntax Description	<i>type</i>	(Optional) Interface type supported on your router.
	<i>number</i>	(Optional) Port number of the interface. The syntax varies depending on the type of router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash marks are required). Refer to the appropriate hardware manual for numbering information.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines	<p>The show interface mac command displays information for one interface, when specified, or all interfaces configured for MAC accounting.</p> <p>For incoming packets on the interface, the accounting statistics are gathered before the committed access rate (CAR)/distributed committed access rate (DCAR) functionality is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after the CAR output, and before DCAR output or distributed weighted random early detection (DWRED) or distributed weighted fair queuing (DWFQ) functionality is performed on the packet.</p> <p>Therefore, if DCAR or DWRED is performed on the interface and packets are dropped, the dropped packets are still counted in the show interface mac command.</p> <p>The maximum number of MAC addresses that can be stored for the input and output addresses is 512 each. After the maximum is reached, subsequent MAC addresses are ignored.</p> <p>To clear the accounting statistics, use the clear counter EXEC command. To configure an interface for IP accounting based on the MAC address, use the ip accounting mac-address interface configuration command.</p>
------------------	--

Examples

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

```
Router# show interface ethernet 0/1/1 mac

Ethernet0/1/1
  Input (511 free)
    0007.f618.4449(228): 4 packets, 456 bytes, last: 2684ms ago
                    Total: 4 packets, 456 bytes
  Output (511 free)
    0007.f618.4449(228): 4 packets, 456 bytes, last: 2692ms ago
                    Total: 4 packets, 456 bytes
```

Table 5 describes the significant fields shown in the display.

Table 5 *show interface mac Field Descriptions*

Field	Description
Ethernet0/1/1	Interface type and number.
Input Output	Number of packets received as input or sent as output by this interface.
0007.f618.4449(228)	MAC address of the interface from or to which this router sends or receives packets.
packets	Total number of messages that have been transmitted or received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted or received by the system.
last	Time, in milliseconds, since the last IP packet was transmitted or received on the specified interface.

Related Commands

Command	Description
ip accounting mac-address	Enables IP accounting on any interface based on the source and destination MAC address.

show interface precedence

To display precedence accounting information for interfaces configured for precedence accounting, use the **show interface precedence** command in user EXEC or privileged EXEC mode.

show interface [*type number*] **precedence**

Syntax Description	<i>type</i>	(Optional) Interface type supported on your router.
	<i>number</i>	(Optional) Port number of the interface. The syntax varies depending on the type of router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash is required). Refer to the appropriate hardware manual for numbering information.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines The **show interface precedence** command displays information for one interface, when specified, or all interfaces configured for IP precedence accounting.

For incoming packets on the interface, the accounting statistics are gathered before the committed access rate (CAR)/distributed committed access rate (DCAR) functionality is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after the CAR output, and before DCAR output or distributed weighted random early detection (DWRED) or distributed weighted fair queuing (DWFQ) functionality is performed on the packet. Therefore, if DCAR or DWRED is performed on the interface and packets are dropped, the dropped packets are still counted in the **show interface mac** command.

To clear the accounting statistics, use the **clear counter EXEC** command.

To configure an interface for IP accounting based on IP precedence, use the **ip accounting precedence** interface configuration command.

Examples

The following is sample output from the **show interface precedence** command. In this example, the total packet and byte counts are calculated for the interface that receives (input) or sends (output) IP packets and sorts the results based on IP precedence.

```
Router# show interface ethernet 0/1/1 precedence
```

```
Ethernet0/1/1
  Input
    Precedence 0:  4 packets, 456 bytes
  Output
    Precedence 0:  4 packets, 456 bytes
```

Table 6 describes the fields shown in the display.

Table 6 *show interface precedence Field Descriptions*

Field	Description
Ethernet0/1/1	Interface type and number.
Input Output	An interface that receives or sends IP packets and sorts the results based on IP precedence.
Precedence	Precedence value for the specified interface.
packets	Total number of messages that have been transmitted or received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted or received by the system.

Related Commands

Command	Description
ip accounting precedence	Enables IP accounting on any interface based on IP precedence.

show ip access-list

To display the contents of all current IP access lists, use the **show ip access-list** command in user EXEC or privileged EXEC mode.

```
show ip access-list [access-list-number | access-list-name]
```

Syntax Description

access-list-number (Optional) Number of the IP access list to display.

access-list-name (Optional) Name of the IP access list to display.

Defaults

Displays all standard and extended IP access lists.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

The **show ip access-list** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-list** command when all access lists are requested:

```
Router# show ip access-list

Extended IP access list 101
  deny udp any any eq ntp
  permit tcp any any
  permit udp any any eq tftp
  permit icmp any any
  permit udp any any eq domain
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Router# show ip access-list Internetfilter

Extended IP access list Internetfilter
  permit tcp any 171.69.0.0 0.0.255.255 eq telnet
  deny tcp any any
  deny udp any 171.69.0.0 0.0.255.255 lt 1024
  deny ip any any log
```

show ip accounting

To display the active accounting or checkpointed database or to display access list violations, use the **show ip accounting** command in user EXEC or privileged EXEC mode.

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

Syntax Description	Parameter	Description
	checkpoint	(Optional) Indicates that the checkpointed database should be displayed.
	output-packets	(Optional) Indicates that information pertaining to packets that passed access control and were routed should be displayed. If neither the output-packets nor access-violations keyword is specified, output-packets is the default.
	access-violations	(Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. If neither the output-packets nor access-violations keyword is specified, output-packets is the default.

Defaults

If neither the **output-packets** nor **access-violations** keyword is specified, the **show ip accounting** command displays information pertaining to packets that passed access control and were routed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
10.3	The output-packets and access-violations keywords were added.

Usage Guidelines

If you do not specify any keywords, the **show ip accounting** command displays information about the active accounting database, and traffic coming from a remote site and transiting through a router.

To display IP access violations, you must use the **access-violations** keyword. If you do not specify the keyword, the command defaults to displaying the number of packets that have passed access lists and were routed.

To use this command, you must first enable IP accounting on a per-interface basis.

Examples

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

```
Router# show ip accounting
```

Source	Destination	Packets	Bytes
172.16.19.40	192.168.67.20	7	306
172.16.13.55	192.168.67.20	67	2749
172.16.2.50	192.168.33.51	17	1111
172.16.2.50	172.31.2.1	5	319
172.16.2.50	172.31.1.2	463	30991

```

172.16.19.40 172.16.2.1 4 262
172.16.19.40 172.16.1.2 28 2552
172.16.20.2 172.16.6.100 39 2184
172.16.13.55 172.16.1.2 35 3020
172.16.19.40 192.168.33.51 1986 95091
172.16.2.50 192.168.67.20 233 14908
172.16.13.28 192.168.67.53 390 24817
172.16.13.55 192.168.33.51 214669 9806659
172.16.13.111 172.16.6.23 27739 1126607
172.16.13.44 192.168.33.51 35412 1523980
192.168.7.21 172.163.1.2 11 824
172.16.13.28 192.168.33.2 21 1762
172.16.2.166 192.168.7.130 797 141054
172.16.3.11 192.168.67.53 4 246
192.168.7.21 192.168.33.51 15696 695635
192.168.7.24 192.168.67.20 21 916
172.16.13.111 172.16.10.1 16 1137
accounting threshold exceeded for 7 packets and 433 bytes

```

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

```
Router# show ip accounting access-violations
```

```

Source          Destination      Packets    Bytes     ACL
172.16.19.40    192.168.67.20   7          306      77
172.16.13.55    192.168.67.20   67         2749     185
172.16.2.50     192.168.33.51   17         1111     140
172.16.2.50     172.16.2.1      5          319      140
172.16.19.40    172.16.2.1      4          262      77
Accounting data age is 41

```

The following is sample output from the **show ip accounting** command. The output shows the original source and destination addresses that are separated by three routers:

```
Router3# show ip accounting
```

```

Source          Destination      Packets    Bytes
10.225.231.154 172.16.10.2     44         28160
10.76.97.34     172.16.10.2     44         28160
10.10.11.1      172.16.10.2     507        324480
10.10.10.1      172.16.10.2     507        318396
10.100.45.1     172.16.10.2     508        325120
10.98.32.5      172.16.10.2     44         28160

```

```
Accounting data age is 2
```

[Table 7](#) describes the significant fields shown in the displays.

Table 7 *show ip accounting Field Descriptions*

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets sent from the source address to the destination address. With the access-violations keyword, the number of packets sent from the source address to the destination address that violated an access control list (ACL).

Table 7 *show ip accounting Field Descriptions (continued)*

Field	Description
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets sent from the source address to the destination address. With the access-violations keyword, the total number of bytes sent from the source address to the destination address that violated an ACL.
ACL	Number of the access list of the last packet sent from the source to the destination that failed an access list filter.
accounting threshold exceeded...	Data for all packets that could not be entered into the accounting table when the accounting table is full. This data is combined into a single entry.

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.

show ip aliases

To display the IP addresses mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similarly to aliases, use the **show ip aliases** EXEC command.

show ip aliases

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To distinguish a SLIP address from a normal alias address, the command output uses the form SLIP TTY1 for the “port” number, where 1 is the auxiliary port.

Examples

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

```
Router# show ip aliases

  IP Address      Port
172.16.0.0       SLIP TTY1
```

The display lists the IP address and corresponding port number.

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where Serial Line Internet Protocol (SLIP) addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

```
show ip arp [ip-address] [host-name] [mac-address] [interface type number]
```

Syntax Description

<i>ip-address</i>	(Optional) ARP entries matching this IP address are displayed.
<i>host-name</i>	(Optional) Host name.
<i>mac-address</i>	(Optional) 48-bit MAC address.
<i>interface type number</i>	(Optional) ARP entries learned via this interface type and number are displayed.

Command Modes

EXEC

Command History

Release	Modification
9.0	This command was introduced.

Usage Guidelines

ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

Examples

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

```
Router# show ip arp

Protocol  AddressAge(min)  Hardware Addr  Type   Interface
Internet  172.16.233.2290000.0c59.f892  ARPA    Ethernet0/0
Internet  172.16.233.2180000.0c07.ac00  ARPA    Ethernet0/0
Internet  172.16.233.19-0000.0c63.1300  ARPA    Ethernet0/0
Internet  172.16.233.3090000.0c36.6965  ARPA    Ethernet0/0
Internet  172.16.168.11-0000.0c63.1300  ARPA    Ethernet0/0
Internet  172.16.168.25490000.0c36.6965  ARPA    Ethernet0/0
```

[Table 8](#) describes the significant fields shown in the display.

Table 8 *show ip arp* Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

Table 8 *show ip arp Field Descriptions (continued)*

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: <ul style="list-style-type: none">• ARPA• SNAP• SAP
Interface	Indicates the interface associated with this network address.

show ip casa affinities

To display statistics about affinities, use the **show ip casa affinities** command in user EXEC or privileged EXEC mode.

```
show ip casa affinities [stats] | [saddr ip-address [detail]] | [daddr ip-address [detail]] | sport
source-port [detail] | dport destination-port [detail] | protocol protocol [detail]
```

Syntax Description

stats	(Optional) Displays limited statistics.
saddr <i>ip-address</i>	(Optional) Displays the source address of a given TCP connection.
detail	(Optional) Displays the detailed statistics.
daddr <i>ip-address</i>	(Optional) Displays the destination address of a given TCP connection.
sport <i>source-port</i>	(Optional) Displays the source port of a given TCP connection.
dport <i>destination-port</i>	(Optional) Displays the destination port of a given TCP connection.
protocol <i>protocol</i>	(Optional) Displays the protocol of a given TCP connection.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa affinities** command:

```
Router# show ip casa affinities

                          Affinity Table
Source Address  Port  Dest Address  Port  Prot
172.16.36.118  1118  172.16.56.13  19    TCP
172.16.56.13   19    172.16.118   1118  TCP
```

The following is sample output of the **show ip casa affinities detail** command:

```
Router# show ip casa affinities detail

                          Affinity Table
Source Address  Port  Dest Address  Port  Prot
172.16.36.118  1118  172.16.56.13  19    TCP
Action Details:
  Interest Addr:          172.26.56.19      Interest Port: 1638
  Interest Packet: 0x0102 SYN FRAG
  Interest Tickle: 0x0005 FIN RST
  Dispatch (Layer 2):    YES          Dispatch Address: 172.16.56.33

Source Address  Port  Dest Address  Port  Prot
172.16.56.13   19    172.16.36.118  1118  TCP
Action Details:
  Interest Addr:          172.16.56.19      Interest Port: 1638
  Interest Packet: 0x0104 RST FRAG
```

```

Interest Tickle: 0x0003 FIN SYN
Dispatch (Layer 2): NO           Dispatch Address: 10.0.0.0

```

Table 9 describes the significant fields shown in the display.

Table 9 *show ip casa affinities Field Descriptions*

Field	Description
Source Address	Source address of a given TCP connection.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Port	Destination of a given TCP connection.
Prot	Protocol of a given TCP connection.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager address that is to receive interest packets for this affinity.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of TCP packet types of interest to the services manager is interested in.
Interest Tickle	List of TCP packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.
show ip casa oper	Displays operational information about the forwarding agent.

show ip casa oper

To display operational information about the forwarding agent, use the **show ip casa oper** command in user EXEC or privileged EXEC mode.

show ip casa oper

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Examples The following is sample output from the **show ip casa oper** command:

```
Router# show ip casa oper

Casa is Active
  Casa control address is 10.10.20.34/32
  Casa multicast address is 239.1.1.1
  Listening for wildcards on:
    Port:1637
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:180 sec (Default)
```

[Table 10](#) describes the significant fields shown in the display.

Table 10 *show ip casa oper Field Descriptions*

Field	Description
Casa is Active	The forwarding agent is active.
Casa control address	Unique address for this forwarding agent.
Casa multicast address	Services manager broadcast address.
Listening for wildcards on	Port on which the forwarding agent will listen.
Port	Services manager broadcast port.
Current passwd	Current password.
Pending passwd	Password that will override the current password.
Passwd timeout	Interval after which the pending password becomes the current password.

Related Commands	Command	Description
	ip casa oper	Configures the router to function as an MNLB forwarding agent.

show ip casa stats

To display statistical information about the Forwarding Agent, use the **show ip casa stats** command in user EXEC or privileged EXEC mode.

show ip casa stats

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following is sample output of the **show ip casa stats** command:

```
Router# show ip casa stats

Casa is active:
  Wildcard Stats:
    Wildcards:          6          Max Wildcards:    6
    Wildcard Denies:    0          Wildcard Drops:   0
    Pkts Throughput: 441          Bytes Throughput: 39120
  Affinity Stats:
    Affinities:         2          Max Affinities:   2
    Cache Hits:         444         Cache Misses:     0
    Affinity Drops:    0
  Casa Stats:
    Int Packet:         4          Int Tickle:       0
    Casa Denies:        0          Drop Count:       0
```

[Table 11](#) describes the significant fields shown in the display.

Table 11 *show ip casa stats Field Descriptions*

Field	Description
Casa is Active	The Forwarding Agent is active.
Wildcard Stats	Wildcard statistics.
Wildcards	Number of current wildcards.
Max Wildcards	Maximum number of wildcards since the Forwarding Agent became active.
Wildcard Denies	Protocol violations.
Wildcard Drops	Not enough memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.
Bytes Throughput	Number of bytes passed through all wildcards.

Table 11 *show ip casa stats Field Descriptions (continued)*

Field	Description
Affinity Stats	Affinity statistics.
Affinities	Current number of affinities.
Max Affinities	Maximum number of affinities since the forwarding agent became active.
Cache Hits	Number of packets that match wildcards and fixed affinities.
Cache Misses	Matched wildcard, missed fix.
Affinity Drops	Number of times an affinity could not be created.
Casa Stats	Forwarding agent statistics.
Int Packet	Interest packets.
Int Tickle	Interest tickles.
Casa Denies	Protocol violation.
Security Drops	Packets dropped due to password or authentication mismatch.
Drop Count	Number of messages dropped.

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

show ip casa wildcard

To display information about wildcard blocks, use the **show ip casa wildcard** command in user EXEC or privileged EXEC mode.

show ip casa wildcard [detail]

Syntax Description	detail	(Optional) Displays detailed statistics.
--------------------	--------	--

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Examples

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

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

```
Router# show ip casa wildcard
```

Source Address	Source Mask	Port	Dest Address	Dest Mask	Port	Prot
10.0.0.0	0.0.0.0	0	172.16.56.2	255.255.255.255	0	ICMP
10.0.0.0	0.0.0.0	0	172.16.56.2	255.255.255.255	0	TCP
10.0.0.0	0.0.0.0	0	172.16.56.13	255.255.255.255	0	ICMP
10.0.0.0	0.0.0.0	0	172.16.56.13	255.255.255.255	0	TCP
172.16.56.2	255.255.255.255	0	10.0.0.0	0.0.0.0	0	TCP
172.16.56.13	255.255.255.255	0	10.0.0.0	0.0.0.0	0	TCP

The following is sample output from the **show ip casa wildcard detail** command:

```
Router# show ip casa wildcard detail
```

Source Address	Source Mask	Port	Dest Address	Dest Mask	Port	Prot
10.0.0.0	0.0.0.0	0	172.16.56.2	255.255.255.255	0	ICMP

Service Manager Details:

Manager Addr: 172.16.56.19 Insert Time: 08:21:27 UTC 04/18/96

Affinity Statistics:

Affinity Count: 0 Interest Packet Timeouts: 0

Packet Statistics:

Packets: 0 Bytes: 0

Action Details:

Interest Addr: 172.16.56.19 Interest Port: 1638

Interest Packet: 0x8000 ALLPKTS

Interest Tickle: 0x0107 FIN SYN RST FRAG

Dispatch (Layer 2): NO Dispatch Address: 10.0.0.0

Advertise Dest Address: YES Match Fragments: NO

Source Address	Source Mask	Port	Dest Address	Dest Mask	Port	Prot
10.0.0.0	0.0.0.0	0	172.16.56.2	255.255.255.255	0	TCP

Service Manager Details:

Manager Addr: 172.16.56.19 Insert Time: 08:21:27 UTC 04/18/96

Affinity Statistics:

show ip casa wildcard

```

Affinity Count:          0          Interest Packet Timeouts: 0
Packet Statistics:
Packets:                0          Bytes: 0
Action Details:
Interest Addr:          172.16.56.19  Interest Port: 1638
Interest Packet: 0x8102 SYN FRAG ALLPKTS
Interest Tickle: 0x0005 FIN RST
Dispatch (Layer 2):     NO          Dispatch Address: 10.0.0.0
Advertise Dest Address: YES        Match Fragments: NO

```

**Note**

If a filter is not set, the filter is not active.

Table 12 describes significant fields shown in the display.

Table 12 show ip casa wildcard Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Source Mask	Mask to apply to source address before matching.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Dest Mask	Mask to apply to destination address before matching.
Port	Destination port of a given TCP connection.
Prot	Protocol of a given TCP connection.
Service Manager Details	Services manager details.
Manager Addr	Source address of this wildcard.
Insert Time	System time at which this wildcard was inserted.
Affinity Statistics	Affinity statistics.
Affinity Count	Number of affinities created on behalf of this wildcard.
Interest Packet Timeouts	Number of unanswered interest packets.
Packet Statistics	Packet statistics.
Packets	Number of packets that match this wildcard.
Bytes	Number of bytes that match this wildcard.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.
Interest Tickle	List of packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.
Advertise Dest Address	Destination address.
Match Fragments	Does wildcard also match fragments? (boolean)

Related Commands	Command	Description
	show ip casa oper	Displays operational information about the Forwarding Agent.

show ip dhcp binding

To display address bindings on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp binding** command in user or privileged EXEC mode.

```
show ip dhcp binding [ip-address]
```

Syntax Description	<i>ip-address</i>	(Optional) Specifies the IP address of the DHCP client for which bindings will be displayed.
---------------------------	-------------------	--

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.0(15)T	Support to display allocated subnets was added to the output.

Usage Guidelines	This command is used to display DHCP binding information for IP address assignment and subnet allocation. If the address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed. The output from this command displays binding information for individual IP address assignment and allocated subnets. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address only display an IP address and are not followed by a subnet mask.
-------------------------	---

Examples

IP Address Assignment Example

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, and the type of address assignment that have occurred. [Table 13](#) lists descriptions of the fields in each example.

```
Router# show ip dhcp binding 172.16.1.11
```

IP address	Hardware address	Lease expiration	Type
172.16.1.11	00a0.9802.32de	Feb 01 1998 12:00 AM	Automatic

```
Router# show ip dhcp binding 172.16.3.254
```

IP address	Hardware address	Lease expiration	Type
172.16.3.254	02c7.f800.0422	Infinite	Manual

Table 13 *show ip dhcp binding Field Descriptions*

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Subnet Allocation Example

The following example shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default). The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet) in CIDR bit count notation. Bindings for an individual IP address only display an IP address and are not followed by a subnet mask. [Table 14](#) lists descriptions of the fields in each example.

```
Router# show ip dhcp binding
```

```
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration      Type
                Hardware address/
                User name
10.0.0.0/26     0063.6973.636f.2d64.   Mar 29 2003 04:36 AM   Automatic
                656d.6574.6572.2d47.
                4c4f.4241.4c
```

Table 14 *show ip dhcp binding Field Descriptions*

Field	Description
IP address	The IP address of the host as recorded on the DHCP server. The subnet that follows the IP address (/26) in the example defines this binding as a subnet allocation binding.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.

show ip dhcp conflict

To display address conflicts found by a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server when addresses are offered to the client, use the **show ip dhcp conflict** command in user EXEC or privileged EXEC mode.

show ip dhcp conflict [*ip-address*]

Syntax Description

ip-address (Optional) Specifies the IP address of the conflict found.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The server uses ping to detect conflicts. The client uses gratuitous Address Resolution Protocol (ARP) to detect clients. If an address conflict is detected, the address is removed from the pool and the address is not assigned until an administrator resolves the conflict.

Examples

The following example displays the detection method and detection time for all IP addresses the DHCP server has offered that have conflicts with other devices. [Table 15](#) lists descriptions of the fields in the example.

```
Router# show ip dhcp conflict

IP address      Detection Method  Detection time
172.16.1.32     Ping              Feb 16 1998 12:28 PM
172.16.1.64     Gratuitous ARP    Feb 23 1998 08:12 AM
```

Table 15 show ip dhcp conflict Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP server. Can be a ping or a gratuitous ARP.
Detection time	The date and time when the conflict was found.

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.

Command	Description
ip dhcp ping packets	Specifies the number of packets a Cisco IOS DHCP server sends to a pool address as part of a ping operation.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP server waits for a ping reply from an address pool.

show ip dhcp database

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database agent information, use the **show ip dhcp database** command in privileged EXEC mode.

show ip dhcp database [*url*]

Syntax Description

<i>url</i>	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
------------	--

Defaults

If a URL is not specified, all database agent records are shown. Otherwise, only information about the specified agent is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.

Examples

The following example shows all DHCP server database agent information. [Table 16](#) lists descriptions for each field in the example.

```
Router# show ip dhcp database

URL       : ftp://user:password@172.16.4.253/router-dhcp
Read      : Dec 01 1997 12:01 AM
Written   : Never
Status    : Last read succeeded. Bindings have been loaded in RAM.
Delay     : 300 seconds
Timeout   : 300 seconds
Failures  : 0
Successes : 1
```

Table 16 *show ip dhcp database Field Descriptions*

Field	Description
URL	Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
Read	The last date and time bindings were read from the file server.
Written	The last date and time bindings were written to the file server.
Status	Indication of whether the last read or write of host bindings was successful.
Delay	The amount of time (in seconds) to wait before updating the database.
Timeout	The amount of time (in seconds) before the file transfer is aborted.
Failures	The number of failed file transfers.
Successes	The number of successful file transfers.

Related Commands

Command	Description
ip dhcp database	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.

show ip dhcp import

To display the option parameters that were imported into the Dynamic Host Configuration Protocol (DHCP) server database, use the **show ip dhcp import** command in privileged EXEC command.

show ip dhcp import

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(2)T	This command was introduced.

Usage Guidelines Imported option parameters are not part of the router configuration and are not saved in NVRAM. Thus, the **show ip dhcp import** command is necessary to display the imported option parameters.

Examples The following is sample output from the **show ip dhcp import** command:

```
Router# show ip dhcp import

Address Pool Name:2
Domain Name Server(s): 1.1.1.1
NetBIOS Name Server(s): 3.3.3.3
```

The following example indicates the address pool name:

```
Address Pool Name:2
```

The following example indicates the imported values, which are domain name and NetBIOS name information:

```
Domain Name Server(s): 1.1.1.1
NetBIOS Name Server(s): 3.3.3.3
```

Related Commands	Command	Description
	import all	Imports option parameters into the DHCP database.
	show ip dhcp database	Displays Cisco IOS server database information.

show ip dhcp pool

To display information about the Dynamic Host Configuration Protocol (DHCP) address pools, use the **show ip dhcp pool** command in privileged EXEC configuration mode.

```
show ip dhcp pool [name]
```

Syntax Description

<i>name</i>	(Optional) Displays information about a specific address pool. If not specified, displays information about all address pools.
-------------	--

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to determine the subnets allocated and to examine the current utilization level for the pool or all the pools if the *name* argument is not used.

Examples

The following example shows DHCP address pool information for pool 1. [Table 17](#) describes the significant fields in the display.

```
Router# show ip dhcp pool 1

Pool 1:
Utilization mark (high/low)      : 85 / 15
Subnet size (first/next)         : 24 / 24 (autogrow)
VRF name                          : abc
Total addresses                  : 28
Leased addresses                 : 11
Pending event                    : none
2 subnets are currently in the pool :
Current index      IP address range      Leased addresses
10.1.1.12         10.1.1.1 - 10.1.1.14      11
10.1.1.17         10.1.1.17 - 10.1.1.30    0
Interface Ethernet0/0 address assignment
10.1.1.1 255.255.255.248
10.1.1.17 255.255.255.248 secondary
```

Table 17 show ip dhcp pool Field Descriptions

Field	Description
Pool 1	The name of the pool.
Utilization mark (high/low)	The configured high and low utilization level for the pool.
Subnet size (first/next)	The size of the requested subnets.
VRF name	The VRF name to which the pool is associated.

Table 17 *show ip dhcp pool Field Descriptions (continued)*

Field	Description
Total addresses	The total number of addresses in the pool.
Leased addresses	The number of leased addresses in the pool.
Pending event	Displays any pending events.
2 subnets are currently in the pool	The number of subnets allocated to the address pool.
Current index	Displays the current index.
IP address range	The IP address range of the subnets.
Leased addresses	The number of leased addresses from each subnet.
Interface Ethernet0/0 address assignment	The first line is the primary IP address of the interface. The second line is the secondary IP address of the interface. More than one secondary address on the interface is supported.

show ip dhcp relay information trusted-sources

To display all interfaces configured to be a trusted source for the Dynamic Host Configuration Protocol (DHCP) relay information option, use the **show ip dhcp relay information trusted-sources** command in EXEC mode.

```
show ip dhcp relay information trusted-sources
```

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following is sample output when the **ip dhcp relay information trusted** interface configuration command is configured. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Router# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
Ethernet1/1      Ethernet1/2      Ethernet1/3      Serial4/1.1
Serial4/1.2      Serial4/1.3
```

The following is sample output when the **ip dhcp relay information trust-all** global configuration command is configured. Note that the display output does not list the individual interfaces.

```
Router# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option
```

Related Commands

Command	Description
ip dhcp relay information trusted	Configures an interface as a trusted source of the DHCP relay agent information option.
ip dhcp relay information trust-all	Configures all interfaces on a router as trusted sources of the DHCP relay agent information option.

show ip dhcp server statistics

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) server statistics, use the **show ip dhcp server statistics** command in privileged EXEC mode.

show ip dhcp server statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Examples The following example displays DHCP server statistics. [Table 18](#) lists descriptions for each field in the example.

```
Router> show ip dhcp server statistics
```

```
Memory usage          40392
Address pools         3
Database agents       1
Automatic bindings   190
Manual bindings       1
Expired bindings      3
Malformed messages   0
Secure arp entries    1

Message              Received
BOOTREQUEST          12
DHCPDISCOVER         200
DHCPPREQUEST         178
DHCPDECLINE          0
DHCPRELEASE          0
DHCPIFORM            0

Message              Sent
BOOTREPLY            12
DHCPOFFER            190
DHCPACK              172
DHCPCNAK             6
```

Table 18 show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.

Table 18 *show ip dhcp server statistics Field Descriptions (continued)*

Field	Description
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Secure arp entries	The number of ARP entries that have been secured to the MAC address of the client interface.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

Related Commands

Command	Description
clear ip dhcp server statistics	Resets all Cisco IOS DHCP server counters.

show ip dns primary

To display the authority record parameters configured for the Domain Name System (DNS) server, use the **show ip dns primary** command in user EXEC or privileged EXEC mode.

show ip dns primary

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.0	This command was introduced.

Examples The following example shows how to configure the router as a DNS server and then display the authority record parameters for the DNS server:

```
Router(conf)# ip dns server
Router(conf)# ip dns primary example.com soa ns1.example.com mb1.example.com
Router(conf)# ip host example.com ns ns1.example.com
Router(conf)# ip host ns1.example.com 209.165.201.1
Router(conf)# exit
Router# show ip dns primary
Primary for zone example.com:
  SOA information:
    Zone primary (MNAME): ns1.example.com
    Zone contact (RNAME): mb1.example.com
    Refresh (seconds):    21600
    Retry (seconds):      900
    Expire (seconds):     7776000
    Minimum (seconds):    86400
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip dns primary Field Descriptions

Field	Description
Zone primary (MNAME)	Authoritative name server.
Zone contact (RNAME)	DNS mailbox of administrative contact.
Refresh (seconds)	Refresh time in seconds. This time interval that must elapse between each poll of the primary by the secondary name server.
Retry (seconds)	Refresh retry time in seconds. This time interval must elapse between successive connection attempts by the secondary to reach the primary name server in case the first attempt failed.

Table 19 *show ip dns primary Field Descriptions (continued)*

Field	Description
Expire (seconds)	Authority expire time in seconds. The secondary expires its data if it cannot reach the primary name server within this time interval.
Minimum (seconds)	Minimum Time to Live (TTL) in seconds for zone information. Other servers should cache data from the name server for this length of time.

Related Commands

Command	Description
ip dns primary	Configures router authority parameters for the DNS name server, for the DNS name server.
ip dns server	Enables the DNS server on the router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

show ip dns statistics

To display packet statistics for the Domain Name System (DNS) server, use the **show ip dns statistics** command in user EXEC or privileged EXEC mode.

show ip dns statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	12.2T	This command was introduced.

Usage Guidelines Use this command to display the number of DNS requests received and dropped by the DNS server and the number of DNS responses sent by the DNS server.

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

```
Router# show ip dns statistics
DNS requests received = 214 ( 212 + 2 )
DNS requests dropped = 2 ( 0 + 2 )
DNS responses replied = 214 ( 212 + 2 )
```

[Table 20](#) describes the significant fields shown in the display.

Table 20 *show ip dns statistics Field Descriptions*

Field	Description
DNS requests received	Total number of DNS requests received by the DNS server. Additional details are displayed in parenthesis: <ul style="list-style-type: none"> Number of UDP packets received Number of TCP packets received
DNS requests dropped	Total number of DNS requests discarded by the DNS server. Additional details are displayed in parenthesis: <ul style="list-style-type: none"> Number of UDP packets dropped Number of TCP packets dropped
DNS responses replied	Total number of DNS responses sent by the DNS server. Additional details are displayed in parenthesis: <ul style="list-style-type: none"> Number of UDP packets dropped Number of TCP packets dropped

show ip drp

To display information about the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **show ip drp** command in user EXEC or privileged EXEC mode.

show ip drp

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.

Examples

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

```
Router# show ip drp
```

```
Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using "test" key-chain
```

[Table 21](#) describes the significant fields shown in the display.

Table 21 *show ip drp* Field Descriptions

Field	Description
director requests	Number of DRP requests that have been received (including any using authentication key-chain encryption that failed).
successful lookups	Number of successful DRP lookups that produced responses.
failures	Number of DRP failures (for various reasons including authentication key-chain encryption failures).

Related Commands

Command	Description
ip drp access-group	Controls the sources of DRP queries to the DRP server agent.
ip drp authentication key-chain	Configures authentication on the DRP server agent for DistributedDirector.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description	
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(3)T	This command was expanded to include the status of ip wccp redirect out and ip wccp redirect exclude add in commands.
	12.2(14)S	This command was expanded to display the status of NetFlow on a subinterface.
	12.2(15)T	The command output enhancements introduced in Cisco IOS Release 12.2(14)S were integrated into Cisco IOS Release 12.2(15)T.
	12.3(6)	The command output was modified to identify the downstream VRF in the output.
	12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
	12.3(14)YM2	This command was modified to show the usability status of interfaces configured for Multi-Processor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface can send and receive packets. If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see information for that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

The **show ip interface brief** command can be used to view a summary of the router interfaces. This command displays the IP address, interface status, and additional information.

Examples

The following examples from Cisco IOS Release 12.3(14)YM2 show:

- Configuration information on interface Gigabit Ethernet0/3, where the IP flow egress feature is configured on the output side (where packets go out of the interface) and the policy route-map named PBR_NAME is configured on the input side (where packets come into the interface).
- Interface information on Gigabit Ethernet interface 0/3 showing that MPF is enabled and that both features are not supported by MPF and are ignored.

The highlighted arrows (for documentation purposes only) show the configured output and input features and the additional MPF interface information.

```
Router# show running-config interface g 0/3
```

```
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress                <== output
 ip policy route-map PBR_NAME  <== input
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

```
Router# show ip interface g 0/3
```

```
GigabitEthernet0/3 is up, line protocol is up
 Internet address is 10.1.1.1/16
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP CEF switching is enabled
 IP Feature Fast switching turbo vector
 IP VPN Flow CEF switching turbo vector
 IP multicast fast switching is enabled
 IP multicast distributed fast switching is disabled
 IP route-cache flags are Fast, CEF
 Router Discovery is disabled
 IP output packet accounting is disabled
 IP access violation accounting is disabled
 TCP/IP header compression is disabled
 RTP/IP header compression is disabled
 Policy routing is enabled, using route map PBR
 Network address translation is disabled
 BGP Policy Mapping is disabled
```

```

IP Multi-Processor Forwarding is enabled <===== MPF information
  IP Input features, "PBR",
    are not supported by MPF and are IGNORED
  IP Output features, "NetFlow",
    are not supported by MPF and are IGNORED

```

The following example identifies a downstream VRF. The highlighted line (for documentation purposes only) identifies the downstream VRF.

```
Router# show ip interface vi 3
```

```

Virtual-Access3 is up, line protocol is up
Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
Broadcast address is 255.255.255.255
Peer address is 10.8.1.1
MTU is 1492 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN CEF switching turbo vector
VPN Routing/Forwarding "U"
Downstream VPN Routing/Forwarding "D"
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled

```

Table 22 describes the significant fields shown in the display.

Table 22 *show ip interface Field Descriptions*

Field	Description
Virtual-Access3 is up	If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Displays the broadcast address.
Peer address is	Displays the peer address.
MTU is	Displays the MTU value set on the interface.
Helper address	Displays a helper address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	Specifies the IP Security Option (IPSO) security level set for this interface.
Split horizon	Indicates that split horizon is enabled.
ICMP redirects	Specifies whether redirect messages will be sent on this interface.
ICMP unreachable	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Specifies whether Flow switching is enabled for this interface.
IP CEF switching	Specifies whether Cisco Express Forwarding is enabled for the interface.
Downstream VPN Routing/Forwarding “D”	Specifies the VRF where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Specifies whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Specifies whether NetFlow has been enabled on an interface. Displays “Flow init” to specify that NetFlow is enabled on the interface. Displays “Ingress Flow” to specify that NetFlow is enabled on a subinterface using the ip flow ingress command. Specifies “Flow” to specify that NetFlow is enabled on a main interface using the ip route-cache flow command.

Table 22 *show ip interface Field Descriptions (continued)*

Field	Description
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
WCCP Redirect outbound is disabled	Indicates the status of whether packets received on an interface are redirected to a cache engine. Displays “enabled” or “disabled.”
WCCP Redirect exclude is disabled	Indicates the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays “enabled” or “disabled.”

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

```
Router# show ip interface brief
```

```
Interface      IP-Address      OK? Method Status Protocol
Ethernet0      10.108.00.5    YES NVRAM  up      up
Ethernet1      unassigned      YES unset  administratively down down
Loopback0      10.108.200.5   YES NVRAM  up      up
Serial0        10.108.100.5   YES NVRAM  up      up
Serial1        10.108.40.5    YES NVRAM  up      up
Serial2        10.108.100.5   YES manual up      up
Serial3        unassigned      YES unset  administratively down down
```

Table 23 *show ip interface brief Field Descriptions*

Field	Description
Interface	Type of interface.
IP-Address	IP Address assigned to the interface.
OK?	“Yes” means that the IP Address is currently valid. “No” means that the IP Address is not currently valid.

Table 23 *show ip interface brief Field Descriptions (continued)*

Field	Description
Method	<p>The method field has the following possible values:</p> <ul style="list-style-type: none"> • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request • BOOTP—Bootstrap protocol • TFTP—Configuration file obtained from TFTP server • manual—Manually changed by CLI command • NVRAM—Configuration file in NVRAM • IPCP—ip address negotiated command • DHCP—ip address dhcp command • unassigned—No IP address • unset—Unset • other—Unknown
Status	<p>Indicates the status of interface. Valid values and their meanings are:</p> <ul style="list-style-type: none"> • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	Indicates the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ip irdp

To display ICMP Router Discovery Protocol (HRDP) values, use the **show ip irdp** EXEC command.

show ip irdp

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

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

```
Router# show ip irdp

Ethernet 0 has router discovery enabled

Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
--More--
Serial 0 has router discovery disabled
--More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less obvious lines of output in the display are as follows:

Advertisements will occur between every 450 and 600 seconds.

This indicates the configured minimum and maximum advertising interval for the interface.

Advertisements are valid for 1800 seconds.

This indicates the configured holdtime values for the interface.

Default preference will be 100.

This indicates the configured (or in this case default) preference value for the interface.

Related Commands	Command	Description
	ip irdp	Enables IRDP processing on an interface.

show ip masks

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks EXEC** command.

```
show ip masks address
```

Syntax Description	<i>address</i>	Network address for which a mask is required.
---------------------------	----------------	---

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The **show ip masks** command is useful for debugging when a variable-length subnet mask (VLSM) is used. It shows the number of masks associated with the network and the number of routes for each mask.

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

```
Router# show ip masks 172.16.0.0

Mask           Reference count
255.255.255.255 2
255.255.255.0   3
255.255.0.0     1
```

show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics EXEC** command.

show ip nat statistics

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

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

```
Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
  pool net-208: netmask 255.255.255.240
    start 172.16.233.208 end 172.16.233.221
    type generic, total addresses 14, allocated 2 (14%), misses 0
```

[Table 24](#) describes the significant fields shown in the display.

Table 24 *show ip nat statistics Field Descriptions*

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the ip nat outside command.
Inside interfaces	List of interfaces marked as inside with the ip nat inside command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.

Table 24 *show ip nat statistics Field Descriptions (continued)*

Field	Description
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat translations	Displays active NAT translations.

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in EXEC mode.

show ip nat translations [**esp**] [**icmp**] [**pptp**] [**tcp**] [**udp**] [**verbose**] [**vrf** *vrf-name*]

Syntax Description

esp	(Optional) Displays Encapsulating Security Payload (ESP) entries.
icmp	(Optional) Displays Internet Control Message Protocol (ICMP) entries.
pptp	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) entries.
tcp	(Optional) Displays TCP protocol entries.
udp	(Optional) Displays User Datagram Protocol (UDP) entries.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
vrf <i>vrf-name</i>	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The vrf <i>vrf-name</i> keyword and argument combination was added.
12.2(15)T	The esp keyword was added.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
--- 171.16.233.209     192.168.1.95     ---                ---
--- 171.16.233.210     192.168.1.89     ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
udp 172.16.233.209:1220 192.168.1.95:1220 172.16.2.132:53    172.16.2.132:53
tcp 172.16.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
tcp 172.16.233.209:1067 192.168.1.95:1067 172.16.1.161:23    172.16.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ip nat translations verbose
```

```

Pro Inside global      Inside local      Outside local      Outside global
udp 172.16.233.209:1220 192.168.1.95:1220 172.16.2.132:53    172.16.2.132:53
      create 00:00:02, use 00:00:00, flags: extended
tcp 172.16.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
      create 00:01:13, use 00:00:50, flags: extended
tcp 172.16.233.209:1067 192.168.1.95:1067 172.16.1.161:23    172.16.1.161:23
      create 00:00:02, use 00:00:00, flags: extended

```

The following is sample output that includes the **vrf** keyword:

```

Router# show ip nat translations vrf red
Pro Inside global      Inside local      Outside local      Outside global
--- 10.2.2.1           192.168.121.113  ---              ---
--- 10.2.2.2           192.168.122.49  ---              ---
--- 10.2.2.11          192.168.11.1    ---              ---
--- 10.2.2.12          192.168.11.3    ---              ---
--- 20.2.2.13          172.16.5.20     ---              ---

Pro Inside global      Inside local      Outside local      Outside global
--- 10.2.2.3           192.168.121.113  ---              ---
--- 10.2.2.4           192.168.22.49   ---              ---

```

The following is sample output that includes the **esp** keyword:

```

Router# show ip nat translations esp
Pro Inside global      Inside local      Outside local      Outside global
esp 192.168.22.40:0    192.168.122.20:0 192.168.22.20:0
192.168.22.20:28726CD9
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0

```

The following is sample output that includes the **esp** and **verbose** keywords:

```

Router# show ip nat translation esp verbose
Pro Inside global      Inside local      Outside local      Outside global
esp 192.168.22.40:0    192.168.122.20:0 192.168.22.20:0
192.168.22.20:28726CD9
      create 00:00:00, use 00:00:00,
      flags:
      extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0
      create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
      flags:
      extended, use_count:0, entry-id:191, lc_entries:0

```

Table 25 describes the significant fields shown in the display.

Table 25 show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.

Table 25 *show ip nat translations Field Descriptions (continued)*

Field	Description
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: <ul style="list-style-type: none"> • extended—Extended translation • static—Static translation • destination—Rotary translation • outside—Outside translation • timing out—Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.