reserved-only through show ip irdp

reserved-only

To restrict address assignments from the Dynamic Host Configuration Protocol (DHCP) address pool only to the preconfigured reservations, use the **reserved-only** command in DHCP pool configuration mode. To disable the configuration, use the **no** form of this command.

reserved-only

no reserved-only

Syntax Description

This command has no arguments or keywords.

Command Default

Address assignments from the DHCP address pool are not restricted only to the preconfigured reservations.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.2(50)SE	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

When the DHCP port-based assignment feature is configured on multiple switches, devices connected to one switch may receive an IP address assignment from the neighboring switches rather than from the local DHCP address pool switch. If you want the switch to serve only the client directly connected to the switch, you can configure a group of switches with pools that share a common IP subnet but ignore the requests from other clients (not connected to this switch).

Command Examples

The following example shows how to restrict address assignments from the DHCP address pool only to the preconfigured reservations:

```
Router# configure terminal
Router(config)# ip dhcp pool red
Router(dhcp-config)# reserved-only
```

Related Commands

Command	Description
address client-id	Reserves an IP address for a DHCP client identified by client identifier.
address hardware-address	Reserves an IP address for a client identified by hardware address.

restrict authenticated

To specify that a Domain Name System (DNS) view list member cannot be used to respond to an incoming DNS query if the DNS view and the DNS client have not been authenticated, use the **restrict authenticated** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict authenticated

no restrict authenticated

Syntax Description

This command has no arguments or keywords.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the DNS view and the DNS client have been authenticated.

Command Modes

DNS view list member configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query unless the Cisco IOS software has verified the authentication status of the client. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if the client is not authenticated. The router that is running Split DNS determines the query client authentication status by calling any DNS client authentication functions that have been registered with Split DNS.

A client can be authenticated within a Cisco IOS environment by various methods, such as Firewall Authentication Proxy, 802.1x, and wireless authentication. Some DNS authentication functions might inspect only the source IP address or MAC address and the VRF information, while other functions might inspect the source IP address or MAC address, the VRF information, and the DNS view name.

Note In Cisco IOS Release 12.4(9)T, none of these authentication methods are implemented by any Cisco IOS authentication subsystems. As a result, if a DNS view is configured to be restricted based on client authentication, the Cisco IOS software will not use that view whenever the view is considered for handling a query. In future Cisco IOS releases, authentication subsystems will implement client authentication functions and enable them to be registered on a router running Split DNS. This will enable the Cisco IOS software to support authentication-based use restrictions on DNS views. This command is provided now for backward compatibility when DNS authentication functions are implemented.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the query source IP address (configured by using the **restrict source access-group** command) or the query hostname (configured by using the **restrict name-group** command).

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Command Examples

The following example shows how to create the DNS view list userlist5 so that it contains the two DNS views:

```
Router(config)# ip dns view-list userlist5
Router(cfg-dns-view-list)# view vrf vpn101 user1 20
Router(cfg-dns-view-list-member)# exit
Router(cfg-dns-view-list)# view vrf vpn201 user2 35
Router(cfg-dns-view-list-member)# restrict authenticated
```

Both view list members are restricted from responding to an incoming DNS query unless the query is from the same VRF as the VRF with which the view is associated.

The first view list member (the view named user1 and associated with the VRF vpn101) has no further restrictions placed on its use.

The second view list member (the view named user2 and associated with the VRF vpn201) is further restricted from responding to an incoming DNS query unless the Cisco IOS software can verify the authentication status of the client.

Related Commands

Command	Description
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.

Command	Description
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

restrict name-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the query hostname matches a permit clause in a particular DNS name list and none of the deny clauses, use the **restrict name-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict name-group *name-list-number*

no restrict name-group *name-list-number*

Syntax Description

name-list-number	Integer from 1 to 500 that identifies an existing DNS name list.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the query hostname matches a permit clause in a particular DNS name list.

Command Modes

DNS view list member configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query if a permit clause in the specified DNS name list specifies a regular expression that matches the query hostname. The view list member is rejected, and the view-selection process proceeds to the next view in the view list, if an explicit deny clause in the name list (or the implicit deny clause at the end of the name list) matches the query hostname. To configure a DNS name list, use the **ip dns name-list** command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the source IP address of the incoming DNS query. To configure this type of restriction, use the **restrict source access-group** command.

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source VRF of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Note The *name-list-number* argument referenced in this command is configured using the **ip dns name-list** command. The DNS name list is referred to as a "name list" when it is defined and as a "name group" when it is referenced in other commands.

Command Examples

The following example shows how to specify that DNS view user3 associated with the global VRF, when used as a member of the DNS view list userlist5, cannot be used to respond to an incoming DNS query unless the query hostname matches the DNS name list identified by the number 1:

```
Router(config)# ip dns view-list userlist5

Router(cfg-dns-view-list)# view user3 40
Router(cfg-dns-view-list-member)# restrict name-group 1
```

Related Commands

Command	Description
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.
restrict source access-group	Restricts the use of the DNS view list member to DNS queries for which the query source IP address matches a particular standard ACL.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

restrict source access-group

To specify that a Domain Name System (DNS) view list member cannot be used to respond to a DNS query unless the source IP address of the DNS query matches a standard access control list (ACL), use the **restrict source access-group** command in DNS view list member configuration mode. To remove this restriction from a DNS view list member, use the **no** form of this command.

restrict source access-group {*acl-name* | *acl-number*}

no restrict source access-group {*acl-name* | *acl-number*}

Syntax Description

acl-name	String (not to exceed 64 characters) that specifies a standard ACL.
acl-number	Integer from 1 to 99 that specifies a standard ACL.

Command Default

When determining whether the DNS view list member can be used to respond to an incoming DNS query, the Cisco IOS software does not check that the source IP address of the DNS query belongs to a particular standard ACL.

Command Modes

DNS view list member configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command restricts the DNS view list member from responding to an incoming DNS query if the query source IP address matches the specified standard ACL. To configure a standard ACL, use the **access-list** (IP standard) command.

A DNS view list member can also be restricted from responding to an incoming DNS query based on the the query hostname. To configure this type of restriction, use the **restrict name-group** command.

Note If a DNS view list member is configured with multiple usage restrictions, that DNS view can be used to respond to a DNS query only if the view is associated with the source Virtual Private Network (VPN) routing and forwarding (VRF) instance of the query and all configured usage restrictions are met by the query.

To display the usage restrictions for a DNS view list member, use the **show ip dns view-list** command.

Note The *acl-name* or *acl-number* argument referenced in this command is configured using the **access-list** command. The access list is referred to as a "access list" when it is defined and as a "access group" when it is referenced in other commands.

Command Examples

The following example shows how to specify that DNS view user4 associated with the global VRF, when used as a member of the DNS view list userlist7, cannot be used to respond to an incoming DNS query unless the query source IP address matches the standard ACL number 6:

```
Router(config)# ip dns view-list userlist7

Router(cfg-dns-view-list)# view user4 40
Router(cfg-dns-view-list-member)# restrict source access-group 6
```

Related Commands

Command	Description
access-list (IP standard)	Creates a standard ACL that defines the specific host or subnet for host-specific PAM.
restrict name-group	Restricts the use of the DNS view list member to DNS queries for which the query hostname matches a particular DNS name list.
show ip dns view-list	Displays information about a particular DNS view list or about all configured DNS view lists.

service dhcp

To enable the 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 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.

Command Default

DHCP is enabled. DHCP is not running. Port 67 is closed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was modified. Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. This command was broken into two logical parts: service enabled and service running.
12.2SXH	This command was modified. Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. This command was broken into two logical parts: service enabled and service running.

Usage Guidelines

The BOOTP and DHCP servers in Cisco IOS software both use the Internet Control Message Protocol (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.

Port 67 is closed in the Cisco IOS DHCP/BOOTP default configuration. There are two logical parts to the **service dhcp** command: service enabled and service running. The DHCP service is enabled by default, but port 67 is not opened until the DHCP service is running. A DHCP address pool must be configured for the DHCP service to be running. If the service is running, the s**how ip sockets detail or show sockets detail**commands displays port 67 as open.

Command Examples

The following example shows to enable DHCP services on the DHCP server:

```
service dhcp
```

Related Commands

Command	Description
show ip sockets	Displays IP socket information.
show sockets	Displays IP socket information.

set ip next-hop dynamic dhcp

To set the next hop to the gateway that was most recently learned by the Dynamic Host Configuration Protocol (DHCP) client, use the **set ip next-hop dynamic dhcp**command in route-map configuration mode. To restore the default setting, use the **no** form of this command.

set ip next-hop dynamic dhcp

no set ip next-hop dynamic dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-router)

Command History

Release	Modification
12.3(2)XE	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

The **set ip next-hop dynamic dhcp**command supports only a single DHCP interface. If multiple interfaces have DHCP configured, the gateway that was most recently learned among all interfaces running DHCP will be used by the route map.

Command Examples

The following example shows how to configure a local routing policy that sets the next hop to the gateway that was most recently learned by the DHCP client:

```
access list 101 permit icmp any host 172.16.23.7 echo
route map MY-LOCAL-POLICY permit 10
```

```
 match ip address 101
 set ip next-hop dynamic dhcp
!
ip local policy route-map MY-LOCAL-POLICY
```

Related Commands

Command	Description
access list (IP extended)	Defines an extended IP access list.

show arp

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

show arp [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]] **[detail]**

Syntax Description

vrf *vrf-name*	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the *vrf-name* argument. If this option is specified, it can be followed by any valid combination of the *arp-mode*, *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
arp-mode	(Optional) Displays the entries that are in a specific ARP mode. This argument can be replaced by one of the following keywords: • **alias** --Displays only alias ARP entries. An alias ARP entry is a statically configured (permanent) ARP table entry that is associated with a local IP address. This type of entry can be configured or removed using the **arp** (global) command with the **alias** keyword. • **dynamic** --Displays only dynamic ARP entries. A dynamic ARP entry is learned through an ARP request and completed with the MAC address of the external host. • **incomplete** --Displays only incomplete ARP entries. An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host. • **interface** --Displaysonly interface ARP entries. An interface ARP entry contains a local IP address and is derived from an interface. • **static** --Displays only static ARP entries. A static ARP entry is a statically configured (permanent) ARP entry that is associated with an external host. This type of entry can be configured or removed using the **arp** (global) command.

	Note If this option is specified, it can be followed by any valid combination of the *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
ip-address [*mask*]	(Optional) Displays the entries associated with a specific host or network. **Note** If this option is specified, it can be followed by any valid combination of the *interface-type* and *interface-number* arguments and the **detail** keyword.
interface-type interface-number	(Optional) Displays the specified entries that are also associated with this router interface. **Note** If this option is specified, it can be followed by the **detail** keyword.
detail	(Optional) Displays the specified entries with mode-specific details and information about subblocks (if any).

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.4(11)T	The **vrf** keyword and *vrf-name* argument were added to limit the display to entries under a specific VRF. The **alias**, **dynamic**, **incomplete**, **interface**, and **static** keywords were added to limit the display to entries in a specific ARP mode. The *ip-address* and *mask* arguments were added to limit the display to entries for a specific host or network. The *interface-type*and *interface-number* arguments were added to limit the display to entries for a specific interface. The **detail** keyword was added to display additional details about the entries.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To display all entries in the ARP cache, use this command without any arguments or keywords.

Entry Selection Options

You can to limit the scope of the command output by applying various combinations of the following ARP entry selection criteria:

- Entries under a specific VRF
- Entries in a specific ARP mode
- Entries for a specific host or entries for a specific network
- Entries associated with a specific router interface

Tip The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, use the **show interfaces** command with the **summary** keyword. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface-type*and *interface-number* arguments in the **show arp** command.

Detailed Output Format

To include additional details about each ARP entry displayed, use this command with the **detail** keyword. When this display option is used, the following additional information is included:

- Mode-specific details (such as entry update time)
- Subblocks (if any)

ARP Adjacency Notification

If Cisco Express Forwarding (CEF) is enabled on the router, the router maintains forwarding information (outbound interface and MAC header rewrite) for adjacent nodes. A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). CEF stores the forwarding information in an adjacency database so that Layer 2 addressing information can be inserted into link-layer headers attached to the ARP packets.

- To verify that IPv4 CEF is running, use the **show ip cef** command.
- To verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct, use the **show adjacency** command.

The ARP table information is one of the sources for CEF adjacency. Whenever the ARP subsystem attaches an ARP table entry to an outbound interface with a valid hardware address, the subsystem issues an internal “ARP adjacency” notification. The notification causes an ARP background process to synchronize that ARP entry with CEF adjacency via the adjacency database. If the synchronization succeeds, IP ARP adjacency is said to be “installed”; if the synchronization fails, IP ARP adjacency is said to have been “withdrawn.”

Note Attachment to an outbound interface occurs only for ARP entries in the following modes: alias, dynamic, static, Application Simple, and Application Timer.

To display detailed information about any ARP adjacency notification that may have occurred, use the **show arp** command with the **detail** keyword. You can use this information to supplement the information available through ARP/CEF adjacency debug trace. To enable debug trace for ARP/CEF adjacency interactions, use the **debug arp** command with the **adjacency** keyword.

ARP Cache Administration

To refresh all entries for the specified interface (or all interfaces) or to refresh all entries of the specified address (or all addresses) in the specified VRF table (or in the global VRF table), use the **clear arp-cache** command.

To enable debugging output for ARP transactions, use the **debug arp** command.

Command Examples

The following is sample output from the **show arp** command with no optional keywords or arguments specified:

```
Router# show arp

Protocol   Address          Age (min)   Hardware Addr    Type    Interface
Internet   192.0.2.112      120         0000.a710.4baf   ARPA    Ethernet3
AppleTalk  4028.5           29          0000.0c01.0e56   SNAP    Ethernet2
Internet   192.0.2.114      105         0000.a710.859b   ARPA    Ethernet3
AppleTalk  4028.9           -           0000.0c02.a03c   SNAP    Ethernet2
Internet   192.0.2.121      42          0000.a710.68cd   ARPA    Ethernet3
Internet   192.0.2.9        -           0000.3080.6fd4   SNAP    TokenRing0
AppleTalk  4036.9           -           0000.3080.6fd4   SNAP    TokenRing0
Internet   192.0.2.9        -           0000.0c01.7bbd   SNAP    Fddi0
```

The table below describes the fields shown in the display.

Table 1: 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.
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: • ARPA--For Ethernet interfaces. • SAP--For Hewlett-Packard interfaces. • SMDS--For Switched Multimegabit Data Service (SMDS) interfaces. • SNAP--For FDDI and Token Ring interfaces. • SRP-A--For Switch Route Processor, side A (SRP-A) interfaces. • SRP-B--For Switch Route Processor, side B (SRP-B) interfaces.
Interface	Indicates the interface associated with this network address.

When this command is used to display dynamic ARP entries, the display information includes the time of the last update and the amount of time before the next scheduled refresh is to occur. The following is sample output from the **show arp** command for the dynamic ARP entry at network address 192.0.2.1:

```
Router# show arp 192.0.2.1 detail

ARP entry for 192.0.2.1, link type IP.
  Alias, last updated 13323 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is complete, attached to GigabitEthernet1/1.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.1 on GigabitEthernet1/1) was installed.
```

When this command is used to display floating static ARP entries, the display information includes the associated interface, if any.The following is sample output from the **show arp** command for the floating static ARP entry at network address 192.0.2.2 whose intended interface is down:

```
Router# show arp 192.0.2.2 detail

ARP entry for 192.0.2.2, link type IP.
  Alias, last updated 13327 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is incomplete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.2 on GigabitEthernet1/1) was withdrawn.
```

The following is sample detailed output from the **show arp** command for the Application Alias ARP entry at network address 192.0.2.3:

```
Router# show arp 192.0.2.3 detail

ARP entry for 192.0.2.3, link type IP.
  Application Alias, via Ethernet2/2, last updated 0 minute ago.
  Created by "HSRP".
  Encap type is ARPA, hardware address is 0000.0c07.ac02, 6 bytes long.
  ARP subblocks:
  * Application Alias ARP Subblock
  * HSRP
    ARP Application entry for application HSRP.
```

The following is sample detailed output from the **show arp** command for all dynamic ARP entries:

```
Router# show arp dynamic detail

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1, last updated 0 minute ago.
  Encap type is ARPA, hardware address is 0000.0000.0014, 6 bytes long.
  ARP subblocks:
  * Dynamic ARP Subblock
    Entry will be refreshed in 0 minute and 1 second.
    It has 1 chance to be refreshed before it is purged.
    Entry is complete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
debug arp	Enables debugging output for ARP packet transactions.
show adjacency	Verifies that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip cef	Display entries in the FIB or to display a summary of the FIB.

show arp application

To display Address Resolution Protocol (ARP) table information for a specific ARP application or for all applications supported by ARP and running on registered clients, use the **show arp application**command in user EXEC or privileged EXEC mode.

show arp application [*application-id*] **[detail]**

Syntax Description

application-id	(Optional) Displays ARP table information for a specific ARP application. The range is from 200 to 4294967295. If no ID is specified, ARP table information is displayed for all supported ARP applications running on registered clients.
detail	(Optional) Includes detailed information about subblocks for ARP table information displayed (for the specified application or for all applications supported by ARP and running on registered clients).

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

To display ARP table information about all supported ARP applications running on registered clients, use this command without any arguments or keywords.

Entry Selection Options

To display ARP table information about a single ARP application running on a registered client, use this command with the *application-ID*argument.

Detailed Output Format

To display the specified ARP table information along with detailed information about any subblocks, use this command with the **detail** keyword. The additional details consist of the following information:

- IP address or network
- ARP table entry type (dynamic, interface, static, or alias) or ARP application mode (Simple Application or Application Alias)
- Associated interface
- Brief description of the subblock data

Command Examples

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

```
Router# show arp application

Number of clients registered: 7
Application         ID        Num of Subblocks
ARP Backup          200       1
IP SIP              201       0
LEC                 202       0
DHCPD               203       0
IP Mobility         204       0
HSRP                209       1
IP ARP Adjacency    212       2
```

The following is sample detailed output from the **show arp application detail** command:

```
Router# show arp application detail

Number of clients registered: 7
Application         ID        Num of Subblocks
ARP Backup          200       1
ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    Backup for Interface on Ethernet2/2
Application         ID        Num of Subblocks
IP SIP              201       0
Application         ID        Num of Subblocks
LEC                 202       0
Application         ID        Num of Subblocks
DHCPD               203       0
Application         ID        Num of Subblocks
IP Mobility         204       0
Application         ID        Num of Subblocks
HSRP                209       1
ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    ARP Application entry for application HSRP.
Application         ID        Num of Subblocks
IP ARP Adjacency    212       2
ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
ARP entry for 192.0.2.2, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.2 on Ethernet2/1) was installed.
```

The table below describes the significant fields shown in the display.

Table 2: show arp application Field Descriptions

Field	Description
Application	ARP application name

Field	Description
ID	ARP application ID number
Num of Subblocks	Number of subblocks attached

Related Commands

Command	Description
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp ha

To display the status and statistics of Address Resolution Protocol (ARP) high availability (HA), use the **show arp ha** command in user EXEC or privileged EXEC mode.

show arp ha

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use this command to display the ARP HA status and statistics.

HA-Capable Platforms

This command is available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

ARP HA Statistics

The ARP HA process collects one set of statistics for the active RP (described in the show arp ha Field Descriptions for Statistics Collected for an Active RP table below) and a different set of statistics for the standby RP (described in the show arp ha Field Descriptions for Statistics Collected for a Standby RP table below). These statistics can be used to track the RP state transitions when a user is debugging ARP HA issues.

The output from this command depends on the current and most recent states of the RP:

- For the active RP that has been the active RP since the last time the router was rebooted, this command displays the HA statistics for the active RP.
- For the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred, this command displays the HA statistics for the active RP plus the HA statistics collected when the RP was a standby RP.
- For a standby RP, this command displays the HA statistics for a standby RP.

Command Examples

The following is sample output from the **show arp ha** command on the active RP that has been the active RP since the last time the router was rebooted. ARP HA statistics are displayed for the active state only.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP_SYNC).
  2 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  806 synchronization packets sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
```

The following is sample output from the **show arp ha** command on the active RP that had been a standby RP and became the active RP after the most recent SSO occurred. ARP HA statistics are displayed for the active state and also for the previous standby state.

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP).
  1 ARP entry in the synchronization queue.
  1 ARP entry waiting to be synchronized.
  No synchronization packet sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
Statistics collected when ARP HA in standby state:
  No ARP entry in the backup table.
  808 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
  2 ARP entries restored before timer.
  No ARP entry restored on timer.
  No ARP entry purged since interface is down.
  No ARP entry purged on timer.
```

The following is sample output from the **show arp ha** command on the standby RP. ARP HA statistics are displayed for the standby state only.

```
Router# show arp ha

ARP HA in standby state (ARP_HA_ST_S_UP).
  2 ARP entries in the backup table.
  806 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
```

The table below describes the significant fields shown in the display collected for an active RP.

Table 3: show arp ha Field Descriptions for Statistics Collected for an Active RP

Field	Description
ARP HA in active state	The current state that the event-driven state machine contains for the active RP: • ARP_HA_ST_A_BULK--Transient state in which the active RP waits for the standby RP to signal that it has finished processing of the entries sent by the bulk-synchronization operation.

Field	Description
	• ARP_HA_ST_A_SSO--Transient state in which the new active RP waits for the signal to be fully operational. • ARP_HA_ST_A_UP--Active state in which the active RP does not send entries to the standby RP. The active RP transitions into this state either because the standby RP has not come up yet or because a previous synchronization has failed. • ARP_HA_ST_A_UP_SYNC--Active state in which the active RP sends entries from the synchronization queue to the standby RP. The active RP transitions into this state when the number of entries to be synchronized reaches a threshold or when the synchronization timer expires, whichever occurs first.
ARP entries in the synchronization queue	Number of ARP entries that are queued to be synchronized or have already been synchronized to the standby RP. **Note** Entries that have already been synchronized are kept in the synchronization queue in case the standby RP reloads. After the standby RP reboots, the entire queue (including entries that were already synchronized to the standby RP before the reload) must be bulk-synchronized to the standby RP.
ARP entry waiting to be synchronized	Number of ARP entries that are queued to be synchronized to the standby RP.
synchronization packets sent	Number of synchronization packets that have been sent to the standby RP.
error in allocating synchronization packets	Number of errors that occurred while synchronization packets were being allocated.
error in sending synchronization packets.	Number of errors that occurred while synchronization packets were being sent to the standby RP.
error in encoding interface names	Number of errors that occurred while interface names were being encoded.

The table below describes the significant fields shown in the display collected for a standby RP or for an active RP that was previously in the active state.

Table 4: show arp ha Field Descriptions for Statistics Collected for a Standby RP

Field	Description
ARP HA in standby state	The current state that the event-driven state machine contains for the standby RP: • ARP_HA_ST_S_BULK--Transient state in which the standby RP processes the entries sent by the bulk-synchronization operation. After the active RP signals that it has finished sending entries, the standby RP transitions into the ARP_HA_ST_S_UP state and then signals back to the active RP that it has finished processing the entries sent by the bulk-synchronization operation. • ARP_HA_ST_S_UP--Active state in which the standby RP processes the incremental ARP synchronization entries from the active RP. When the switchover occurs, the standby RP transitions to the ARP_HA_ST_A_SSO state.
ARP entries in the backup table	Number of ARP entries contained in the backup ARP table.
synchronization packets processed	Number of synchronization packets that were processed.
synchronization packet dropped in invalid state	Number of synchronization packets that were dropped due to an invalid state.
error in decoding interface names	Number of errors that occurred in decoding interface names.
ARP entries restored before timer	Number of ARP entries that the new active RP restored prior to expiration of the “flush” timer.
ARP entry restored on timer	Number of ARP entries that the new active RP restored upon expiration of the “flush” timer.
ARP entry purged since interface is down	Number of ARP entries that the new active RP purged because the interface went down.
ARP entry purged on timer	Number of ARP entries that the new active RP purged upon expiration of the “flush” timer.

Related Commands

Command	Description
clear arp-cache counters ha	Resets the ARP HA statistics.

Command	Description
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp summary

To display the total number of Address Resolution Protocol (ARP) table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router, use the **show arp summary** command in user EXEC or privileged EXEC mode.

show arp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SRD3	This command was modified. Support was added for the Cisco 7600 router.

Usage Guidelines

Use this command to display high-level statistics about the ARP table entries:

- Total number of ARP table entries
- Number of ARP table entries for each ARP mode
- Number of ARP table entries for each router interface

A maximum limit for learned ARP entries can be configured on the Cisco 7600 platform in Cisco IOS Release 12.2(33)SRD3. This is subject to memory constraints. The 7600 can support a maximum limit of 256,000 learned ARP entries, and if a memory card is installed on the router the maximum limit is extended to 512,000.

Command Examples

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

Note In this example the maximum limit for the number of learned ARP entries has not been configured.

```
Router# show arp summary
```

```
Total number of entries in the ARP table: 10.
Total number of Dynamic ARP entries: 4.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 4.
Total number of Static ARP entries: 2.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Interface Entry Count
Ethernet3/2 1
```

The following is sample output from the **show arp summary**command on a Cisco 7600 router for Cisco IOS Release 12.2(33)SRD3, after a maximum limit is set for the number of learned ARP entries:

```
Router> enable
Router# configure terminal
Router(config)# ip arp entry learn 512000
Router(config)# exit
Router# show arp summary
Total number of entries in the ARP table: 4.
Total number of Dynamic ARP entries: 0.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 3.
Total number of Static ARP entries: 1.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Maximum limit of Learn ARP entry : 512000.
Maximum configured Learn ARP entry limit : 512000.
Learn ARP Entry Threshold is 409600 and Permit Threshold is 486400.
Total number of Learn ARP entries: 0.
Interface              Entry Count
GigabitEthernet4/7               1
GigabitEthernet4/1.1             1
GigabitEthernet4/1               1
EOBC0/0
```

The table below describes the fields shown in the display.

Table 5: show arp summary Command Field Descriptions

Field	Description
Total Number of entries in the ARP table	Displays the number of entries in the ARP table.
Total number of Dynamic ARP entries	Displays the number of ARP entries in the dynamic state.
Total number of Incomplete ARP entries	Displays the number of ARP entries in the incomplete state.
Total number of Interface ARP entries	Displays the number of ARP entries on ARP enabled interfaces.
Total number of Static ARP entries	Displays the number of active statically configured ARP entries.
Total number of Alias ARP entries	Displays the number of active statically configured alias entries.

Field	Description
Total number of Simple Application ARP entries	Displays the number of ARP entries in the simple application mode.
Total number of Application Alias ARP entries	Displays the number of ARP entries in the application alias mode.
Total number of Application Timer ARP entries	Displays the number of ARP entries in the application timer mode.
Maximum limit of Learn ARP entry	Displays the allowed maximum limit for the learned ARP entries.
Maximum configured Learn ARP entry limit	Displays the figure the maximum learned ARP entry limit is set to.
Learn ARP Entry Threshold	Displays the value representing 80 percent of the set maximum learned ARP entry limit.
Permit Threshold	Displays the value representing 95 percent of the set maximum learned ARP entry limit.
Total number of Learn ARP entries	Displays the total number of learned ARP entries.
Interface	Lists the names of the ARP enabled interfaces.
Entry Count	Displays the number of ARP entries on each ARP enabled interface

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
ip arp entry learn	Specifies the maximum number of learned ARP entries.
show arp	Displays ARP table entries.
show arp application	Displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.

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 hostnames and addresses specific to a particular Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

show hosts [**vrf** *vrf-name*] [**view** [*view-name* | **default**]] **[all]** [*hostname* | **summary**]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view *view-name*	(Optional) The *view-name* argument specifies the DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) DNS view associated with the specified or global VRF. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	(Optional) Displays the default view.
all	(Optional) Display all the host tables.
hostname	(Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.
summary	(Optional) The specified hostname cache information is to be displayed in brief summary format. Disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	Support was added for Cisco modem user interface feature.
12.4(4)T	The **vrf**, **all**, and **summary** keywords and *vrf-name* and *hostname* arguments were added.
12.4(9)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

If you specify the **show hosts** command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q key to terminate command output.

Command Examples

The following is sample output from the **show hosts** command with no parameters specified:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the **show hosts** command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101

Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
```

```
Host                      Port  Flags      Age Type   Address(es)
user                      None  (perm, OK)  0   IP    192.0.2.001
www.example.com           None  (perm, OK)  0   IP    192.0.2.111
                                                      192.0.2.112
```

The table below describes the significant fields shown in the display.

Table 6: show hosts Field Descriptions

Field	Description
Default domain	Default domain name to be used to complete unqualified names if no domain list is defined.
Domain list	List of default domain names to be tried in turn to complete unqualified names.
Name/address lookup	Style of name lookup service.
Name servers	List of name server hosts.
Host	Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the **ip hosts** command.
Port	TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.
Flags	Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows: • EX--Entries marked EX are expired. • OK--Entries marked OK are believed to be valid. • perm--A permanent entry is entered by a configuration command and is not timed out. • temp--A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. • ??--Entries marked ?? are considered suspect and subject to revalidation.
Age	Number of hours since the software last referred to the cache entry.
Type	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 hostnames as type HP-IP.

Field	Description
Address(es)	IP address of the host. One host may have up to eight addresses.

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.

show ip aliases

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

show ip aliases

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)T	This command was modified. The output of the command was changed to display the dynamic and interface IP addresses, even when both the IP addresses are the same.

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. The display lists the address type, the IP address, and the corresponding port number. The output field descriptions are self-explanatory.

Command Examples

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

```
Router# show ip aliases
Address Type             IP Address           Port
Interface                10.1.1.1             SLIP TTY1
Dynamic                  198.51.100.1
Dynamic                  198.51.100.22
Dynamic                  10.0.0.0
Dynamic                  10.2.2.2
Interface                10.114.11.39        SLIP TTY1
Interface                172.31.232.182      SLIP TTY1
```

```
Interface               192.0.2.11          SLIP TTY1
Dynamic                 209.165.200.225
Interface               209.165.200.225
```

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

ip-address	(Optional) ARP entries matching this IP address are displayed.
host-name	(Optional) Host name.
mac-address	(Optional) 48-bit MAC address.
interface type number	(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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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.

Command Examples

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

```
Router# show ip arp
Protocol  Address             Age(min)       Hardware Addr     Type      Interface
Internet  172.16.233.229      -              0000.0c59.f892    ARPA      Ethernet0/0
Internet  172.16.233.218      -              0000.0c07.ac00    ARPA      Ethernet0/0
Internet  172.16.233.19       -              0000.0c63.1300    ARPA      Ethernet0/0
Internet  172.16.233.309      -              0000.0c36.6965    ARPA      Ethernet0/0
Internet  172.16.168.11       -              0000.0c63.1300    ARPA      Ethernet0/0
Internet  172.16.168.254      9              0000.0c36.6965    ARPA      Ethernet0/0
```

The table below describes the significant fields shown in the display.

Table 7: 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.
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: • ARPA • SNAP • SAP
Interface	Indicates the interface associated with this network address.

show ip arp inspection

To display the status of DAI for a specific range of VLANs, use the **show ip arp inspection**command in privileged EXEC mode.

show ip arp inspection [**interfaces [interface-name]** | **statistics** [**vlan** *vlan-range*]]

Syntax Description

interfaces *interface-name*	(Optional) Displays the trust state and the rate limit of ARP packets for the provided interface.
statistics	(Optional) Displays statistics for the following types of packets that have been processed by this feature: forwarded, dropped, MAC validation failure, and IP validation failure.
vlan *vlan-range*	(Optional) Displays the statistics for the selected range of VLANs.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not enter the **statistics** keyword, the configuration and operating state of DAI for the selected range of VLANs is displayed.

If you do not specify the interface name, the trust state and rate limit for all applicable interfaces in the system are displayed.

Command Examples

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 3:

```
Router# show ip arp inspection statistics vlan 3
 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
```

```
 ----      ---------        -------     ----------     ----------
    3         31753         102407         102407             0
 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    3         31753              0                    0
 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    3                 0                        0
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs:

```
Router# show ip arp inspection statistics
 Vlan      Forwarded        Dropped     DHCP Drops     ACL Drops
 ----      ---------        -------     ----------     ----------
    1             0              0              0             0
    2             0              0              0             0
    3         68322         220356         220356             0
    4             0              0              0             0
  100             0              0              0             0
  101             0              0              0             0
 1006             0              0              0             0
 1007             0              0              0             0
 Vlan   DHCP Permits    ACL Permits   Source MAC Failures
 ----   ------------    -----------   -------------------
    1             0              0                    0
    2             0              0                    0
    3         68322              0                    0
    4             0              0                    0
  100             0              0                    0
  101             0              0                    0
 1006             0              0                    0
 1007             0              0                    0
 Vlan   Dest MAC Failures   IP Validation Failures
 ----   -----------------   ----------------------
    1                 0                        0
    2                 0                        0
    3                 0                        0
    4                 0                        0
  100                 0                        0
  101                 0                        0
 1006                 0                        0
 1007                 0                        0
```

This example shows how to display the configuration and operating state of DAI for VLAN 1:

```
Router# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active
 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
```

This example shows how to display the trust state of Fast Ethernet interface 6/3:

```
Router# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)    Burst Interval
 ---------------  -----------     ----------    --------------
 Fa6/1            Untrusted               20                 5
```

This example shows how to display the trust state of the interfaces on the switch:

```
Router# show ip arp inspection interfaces
Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Gi1/1            Untrusted               15
 Gi1/2            Untrusted               15
```

```
Gi3/1           Untrusted             15
Gi3/2           Untrusted             15
Fa3/3           Trusted              None
Fa3/4           Untrusted             15
Fa3/5           Untrusted             15
Fa3/6           Untrusted             15
Fa3/7           Untrusted             15
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL for ARP inspection and QoS filtering and enters the ARP ACL configuration submode.
clear ip arp inspection log	Clears the status of the log buffer.
show ip arp inspection	Displays the status of DAI for a specific range of VLANs.

show ip arp inspection log

To show the status of the log buffer, use the **show ip arp inspection log**command in privileged EXEC mode.

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Command Examples

This example shows how to display the current contents of the log buffer before and after the buffers are cleared:

```
Router# show ip arp inspection log
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
 Interface        Vlan   Sender MAC         Sender IP        Num of Pkts
 --------------  -----  -----------------  ---------------  -----------
Fa6/3            1     0002.0002.0002  10.1.1.2          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.3          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.4          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.5          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.6          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.7          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.8          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.9          1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.10         1(12:02:52 UTC Fri Apr 25 2003)
Fa6/3            1     0002.0002.0002  10.1.1.11         1(12:02:52 UTC Fri Apr 25 2003)
    --            --         --               --        5(12:02:52 UTC Fri Apr 25 2003)
```

This example shows how to clear the buffer with the **clear ip arp inspection log** command:

```
Router# clear ip arp inspection log

Router# show ip arp inspection log
```

```
Total Log Buffer Size : 10
Syslog rate : 0 entries per 10 seconds.
No entries in log buffer.
```

Related Commands

Command	Description
clear ip arp inspection log	Clear the status of the log buffer.
show ip arp inspection log	Shows the status of the log buffer.

show ip ddns update

To display information about the Dynamic Domain Name System (DDNS) updates, use the **show ip ddns update**command in privileged EXEC mode.

show ip ddns update [*interface-type number*]

Syntax Description

interface-type number	(Optional) Displays DDNS updates configured on an interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Command Examples

The following output shows the IP DDNS update method on loopback interface 100 and the destination:

```
Router# show ip ddns update
Dynamic DNS Update on Loopback100:
 Update Method Name     Update Destination
 testing                10.1.2.3
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.

show ip ddns update method

To display information about the Dynamic Domain Name System (DDNS) update method, use the **show ip ddns update method**command in privileged EXEC mode.

show ip ddns update method [*method-name*]

Syntax Description

method-name	(Optional) Name of the update method.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Command Examples

The following is sample output from the **show ip ddns update method** command:

```
Router# show ip ddns update method
Dynamic DNS Update Method: test
  Dynamic DNS update in IOS internal name cache
```

Related Commands

Command	Description
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.
show ip ddns update	Displays information about the DDNS updates.
show ip host-list	Displays the assigned hosts in a list.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

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 EXEC or privileged EXEC mode.

Cisco IOS Release 12.0(1)T, 12.2(28)SB, and Later Releases

show ip dhcp binding [*ip-address*]

Cisco IOS Release 12.2(33)SRC and Later 12.2SR Releases

show ip dhcp binding [**vrf** *vrf-name*] [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the DHCP client for which bindings will be displayed. If the *ip-address* argument is used with the **vrf** *vrf-name* option, the binding in the specified VPN routing and forwarding (VRF) instance is displayed.
vrf *vrf-name*	(Optional) Specifies the name of a VRF instance.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(15)T	The command was modified. Support to display allocated subnets was added to the output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SB9	This command was modified. The output was modified to display the option 82 suboptions of the remote ID and circuit ID.

Usage Guidelines

This command is used to display DHCP binding information for IP address assignment and subnet allocation. If a specific IP address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed. 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 display only an IP address and are not followed by a subnet mask.

Command Examples

Examples

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, the type of address assignment that has occurred, and the option 82 suboptions of the remote ID and circuit ID.

The table below describes the significant fields shown in the displays.

```
Router# show ip dhcp binding 192.0.2.2
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2           aabb.cc00.0a00          Apr 28 2010 05:00 AM    Automatic
Remote id : 020a000014000064000000000
```

Table 8: show ip dhcp binding Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Client-ID/Hardware address/User name	The MAC address or client ID 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.
Remote id	Information sent to the DHCP server using a suboption of the remote ID.

Examples

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):

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2/24        0063.6973.636f.2d64.    Mar 29 2003 04:36 AM    Automatic
                    656d.6574.6572.2d47.
                    4c4f.4241.4c
```

The table below describes the significant fields shown in the display.

Table 9: 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 vrf	Displays VRF information on the DHCP server.

show ip dhcp conflict

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

show ip dhcp conflict [*vrf vrf-name*]

Syntax Description

vrf	(Optional) Displays virtual routing and forwarding (VRF) address conflicts found by the DHCP server.
vrf-name	(Optional) The VRF name.

Command Default

If you do not enter the IP address or VRF then all dhcp conflict related information is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

The server uses a ping operation 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.

Command Examples

The following is sample output from the show ip dhcp conflict command, which shows the detection method and detection time for all IP addresses the DHCP server has offered that have conflicts with other devices:

```
Router#
show ip dhcp conflict
IP address    Detection method     Detection time         VRF
172.16.1.32   Ping                 Feb 16 1998 12:28 PM   vrf1
172.16.1.64   Gratuitous ARP       Feb 23 1998 08:12 AM   vrf2
```

The table below describes the fields shown in the display.

Table 10: 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.
VRF	VRFs configured on the DHCP server.

The following is sample output from the **show ip dhcp conflict vrf** command:

```
Router#
show ip dhcp conflict vrf vrf1
IP address        Detection method   Detection time          VRF
172.16.1.32       Ping               Feb 15 2009 05:39 AM    vrf1
```

See the table below for the field description.

Related Commands

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

url	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Command Examples

The following example shows all DHCP server database agent information. The table below describes the significant fields shown in the display.

```
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 11: 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: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.

Command 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): 10.1.1.1
NetBIOS Name Server(s): 10.3.3.3
```

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): 10.1.1.1
NetBIOS Name Server(s): 10.3.3.3
```

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 limit lease

To display the number of times the lease limit threshold has been violated, use the **show ip dhcp limit lease** command in user EXEC or privileged EXEC mode.

show ip dhcp limit lease [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

You can control the number of subscribers at the global level by using the **ip dhcp limit lease per interface** command and at the interface level by using the **ip dhcp limit lease**command. The **show ip dhcp limit lease** command displays the number of lease limit violations per interface or at the global level.

Command Examples

In the following example, the number of lease violations is displayed. If the **ip dhcp limit lease log** command is enabled, the show output will indicate that lease limit logging is enabled:

```
Router# show ip dhcp limit lease
DHCP limit lease logging is enabled
Interface        Count
Serial0/0.1      5
Serial1          3
```

Related Commands

Command	Description
ip dhcp limit lease	Limits the number of leases offered to DHCP clients per interface.

Command	Description
ip dhcp limit lease log	Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded.
ip dhcp limit lease per interface	Limits the number of DHCP leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

show ip dhcp pool

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

show ip dhcp pool [*name*]

Syntax Description

name	(Optional) Name of the address pool.

Command Default

If a pool name is not specified, information about all address pools is displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was modified. The command output was enhanced to display information about excluded addresses in network pools.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

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.

Command Examples

The following example shows DHCP address pool information for an on-demand address pool (ODAP), pool 1. The table below describes the significant fields shown 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
```

The following example shows DHCP address pool information for a network pool, pool 2. The table below describes the significant fields shown in the display.

```
Router# show ip dhcp pool 2
Pool pool2 :
Utilization mark (high/low) : 80 / 70
Subnet size (first/next) : 0 / 0
Total addresses : 256
Leased addresses : 0
Excluded addresses : 2
Pending event : none
2 subnets are currently in the pool:
Current index   IP address range         Leased/Excluded/Total
10.0.2.1        10.0.2.1 - 10.0.2.254     0     / 1     / 254
10.0.4.1        10.0.4.1 - 10.0.4.2       0     / 1     / 2
```

Table 12: show ip dhcp pool Field Descriptions

Field	Description
Pool	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.
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.
Excluded addresses	The number of excluded addresses.
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.

Related Commands

Command	Description
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a DHCP server and enters DHCP pool configuration mode.
ip dhcp subscriber-id interface-name	Automatically generates a subscriber ID value based on the short name of the interface.
ip dhcp use subscriber-id client-id	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.

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 user EXEC or privileged EXEC mode.

show ip dhcp relay information trusted-sources

Syntax Description

This command has no arguments or keywords.

Command Modes

user EXEC privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Command Examples

The following is sample output when the **ip dhcp relay information trusted-sources** 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**globalconfiguration 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 Serial4/1.1
```

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 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 in Cisco IOS Release 12.2(33)SRC and Subsequent 12.2SR Releases

show ip dhcp server statistics [*type number*]

Syntax Description

type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering system for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	The *type* and *number* arguments were added. The command was enhanced to display interface level DHCP statistics.

Command Examples

The following example displays DHCP server statistics. The table below describes the significant fields in the display.

```
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
Renew messages        0
Message               Received
BOOTREQUEST           12
DHCPDISCOVER          200
DHCPREQUEST           178
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0
Message               Sent
BOOTREPLY             12
DHCPOFFER             190
DHCPACK               172
DHCPNAK               6
```

Table 13: 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.
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.
Renew messages	The number of renew messages for a DHCP lease. The counter is incremented when a new renew message has arrived after the first renew message.
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.

Field	Description
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 dhcp snooping

To display the DHCP snooping configuration, use the **show ip dhcp snooping**command in privileged EXEC mode.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Command Examples

This example shows how to display the DHCP snooping configuration:

```
Router# show ip dhcp snooping

Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5 10
Insertion of option 82 is enabled
Interface               Trusted     Rate limit (pps)
--------------------    -------     ----------------
FastEthernet6/11        no          10
FastEthernet6/36        yes         50
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.

Command	Description
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping binding

To display the DHCP snooping binding entries, use the **show ip dhcp snooping binding**command in privileged EXEC mode.

show ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan*] [**interface** *type number*]

Syntax Description

ip-address	(Optional) IP address for the binding entries.
mac-address	(Optional) MAC address for the binding entries.
vlan *vlan*	(Optional) Specifies a valid VLAN number; valid values are from 1 to 4094.
interface *type*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
number	Module and port number.

Command Default

If no argument is specified, the switch displays the entire DHCP snooping binding table.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

DHCP snooping is enabled on a VLAN only if both the global snooping and the VLAN snooping are enabled.

Command Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Router# show ip dhcp snooping binding
MacAddress      IP Address   Lease(seconds)  Type          VLAN   Interface
```

```
-----------     -----------  -------------  -------------  -----  -------------
0000.0100.0201  10.0.0.1     600            dhcp-snooping  100    FastEthernet3/1
```

This example shows how to display an IP address for DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 172.16.101.102
MacAddress      IP Address      Lease (seconds)  Type           VLAN   Interface
-----------     -----------     ---------------  -------------  -----  ------------
0000.0100.0201  172.16.101.102  1600             dhcp-snooping  100    FastEthernet3/1
```

This example shows how to display the MAC address for the DHCP snooping binding entries:

```
Router# show ip dhcp snooping binding 10.5.5.2 0002.b33f.3d5f

MacAddress          IpAddress  Lease(sec)  Type           VLAN  Interface
------------------  ---------  ----------  -------------  ----  ----------------
00:02:B3:3F:3D:5F   10.5.5.2   492         dhcp-snooping  99    FastEthernet6/36 Router#
```

This example shows how to display the DHCP snooping binding entries' MAC address for a specific VLAN:

```
Router# show ip dhcp snooping binding 10.5.5.2 0002.b33f.3d5f vlan 99

MacAddress         IpAddress  Lease(sec)  Type           VLAN  Interface
-----------------  ---------  ----------  -------------  ----  ----------------
00:02:B3:3F:3D:5F  10.5.5.2   479         dhcp-snooping  99    FastEthernet6/36
```

This example shows how to display the DHCP snooping binding entries on VLAN 100:

```
Router# show ip dhcp snooping binding vlan 100
MacAddress         IP Address  Lease(seconds)  Type           VLAN  Interface
-------------      ----------  --------------  -------------  ----  -------------
0000.0100.0201     10.0.0.1    1600            dhcp-snooping  100   FastEthernet3/1
```

This example shows how to display the DHCP snooping binding entries on Fast Ethernet interface 3/1:

```
Router# show ip dhcp snooping binding interface fastethernet3/1
MacAddress         IP Address  Lease(seconds)  Type           VLAN  Interface
-------------      ----------  --------------  -------------  ----  -------------
0000.0100.0201     10.0.0.1    1600            dhcp-snooping  100   FastEthernet3/1
```

The table below describes the fields in the **show ip dhcp snooping** command output.

Table 14: show ip dhcp snooping Command Output

Field	Description
Mac Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; statically configured from CLI or dynamically learned.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping database	Displays the status of the DHCP snooping database agent.

show ip dhcp snooping database

To display the status of the DHCP snooping database agent, use the **show ip dhcp snooping database**command in privileged EXEC mode.

show ip dhcp snooping database [detail]

Syntax Description

detail	(Optional) Provides additional operating state and statistics information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Command Examples

This example shows how to display the DHCP snooping database:

```
Router# show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
```

This example shows how to view additional operating statistics:

```
Router# show ip dhcp snooping database detail

Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
```

```
Abort Timer : 300 seconds
Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running
Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.
Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0
First successful access: Read
Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None
Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping.
ip dhcp snooping binding	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.
ip dhcp snooping limit rate	Configures the number of the DHCP messages that an interface can receive per second.
ip dhcp snooping packets	Enables DHCP snooping on the tunnel interface.
ip dhcp snooping verify mac-address	Verifies that the source MAC address in a DHCP packet matches the client hardware address on an untrusted port.
ip dhcp snooping vlan	Enables DHCP snooping on a VLAN or a group of VLANs.
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding entries.

show ip dhcp vrf

To display the VPN routing and forwarding (VRF) instance information on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp vrf** command in user EXEC or privileged EXEC mode.

show ip dhcp vrf *vrf-name* **binding** {*ip-address* | *****}

Syntax Description

vrf-name	Specifies the VRF name.
binding	Displays DHCP VRF bindings.
ip-address	Specifies the IP address of the DHCP client for which bindings will be displayed.
*****	Displays all bindings in the specified VRF instance.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

This command is used to display VRF information on the Cisco IOS DHCP server. If an IP address is specified, VRF information for the specific client is displayed. If an asterisk (*) is specified, then VRF information for all the clients is displayed.

Command Examples

The following example shows the bindings associated with the VRF instance named red:

```
Router# show ip dhcp vrf red binding *
Bindings from VRF pool red:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.0           0063.6973.636f.2d30.    Mar 11 2007 04:36 AM    Automatic
                    3030.312e.3030.3131.
                    2e30.3032.342d.4574.
                    302f.30
192.0.2.1           0063.6973.636f.2d30.    Mar 11 2007 04:37 AM    Automatic
                    3032.322e.3030.3333.
                    2e30.3034.342d.4574.
                    302f.30
```

The following example shows the bindings associated with a specific IP address in the VRF instance named red:

```
Router# show ip dhcp vrf red binding 192.0.2.2
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.0.2.2           0063.6973.636f.2d30.    Mar 11 2007 04:37 AM    Automatic
                    3032.322e.3030.3333.
                    2e30.3034.342d.4574.
                    302f.30
```

The table below describes the significant fields shown in the displays.

Table 15: show ip dhcp vrf 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.

Related Commands

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

show ip dns name-list

To display a particular Domain Name System (DNS) name list or all configured DNS name lists, use the **show ip dns name-list** command in privileged EXEC mode.

show ip dns name-list [*name-list-number*]

Syntax Description

name-list-number	(Optional) Integer from 1 to 500 that identifies a DNS name list.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Display a DNS name list to view the ordered list of pattern-matching rules it defines. Each rule in the name list specifies a regular expression and the type of action to be taken if the query hostname matches that expression.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Command Examples

The following is sample output from the **show ip dns name-list** command:

```
Router# show ip dns name-list

ip dns name-list 1
deny WWW.EXAMPLE1.COM
permit WWW.EXAMPLE.com
ip dns name-list 2
deny WWW.EXAMPLE2.COM
permit WWW.EXAMPLE3.COM
```

The table below describes the significant fields shown for each DNS name list in the display.

Table 16: show ip dns name-list Field Descriptions

Field	Description
name-list	Integer that identifies the DNS name list. Configured using the **ip dns name-list** command.

Field	Description
deny	Regular expression, case-insensitive, to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name list will be determined to have not matched the hostname. A deny clause is configured by using the **ip dns name-list** command.
permit	Regular expression in domain name format (a sequence of case-insensitive ASCII labels separated by dots), case-insensitive, and to be compared to the DNS query hostname. If the DNS query hostname matches this expression, the name list matching will terminate immediately and the name-list will be determined to have matched the hostname. A permit clause is configured by using the **ip dns name-list** command.

Related Commands

Command	Description
debug ip dns name-list	Enables debugging output for DNS name list events.
ip dns name-list	Defines a list of pattern-matching rules in which each rule permits or denies the use of a DNS view list member to handle a DNS query based on whether the query hostname matches the specified regular expression.

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.

Command 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
```

The table below describes the significant fields shown in the display.

Table 17: 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.

Field	Description
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.
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
12.4(20)T	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.

Command Examples

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

```
Router#
show ip dns statistics
DNS requests received = 818725 ( 818725 + 0 )
DNS requests dropped = 0 ( 0 + 0 )
DNS responses replied = 0 ( 0 + 0 )
Forwarder queue statistics:
Current size = 0
Maximum size = 400
Drops = 804613
Director queue statistics:
Current size = 0
Maximum size = 0
Drops = 0
```

The table below describes the significant fields shown in the display.

Table 18: 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: • Number of UDP packets received

Field	Description
	• Number of TCP packets received
DNS requests dropped	Total number of DNS requests discarded by the DNS server. Additional details are displayed in parenthesis: • 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: • Number of UDP packets dropped • Number of TCP packets dropped
Current size	Displays the current size of the queue counter.
Maximum size	Displays the maximum size of the queue counter reached since the reload. **Note** Whenever you change the queue size, the Maximum size counter will be reset to zero.
Drops	Displays the number of packets dropped when a queue function fails. **Note** Whenever you change the queue size, the Drops counter will be reset to zero.

show ip dns view

To display configuration information about a Domain Name System (DNS) view or about all configured DNS views, including the number of times the DNS view was used, the DNS resolver settings, the DNS forwarder settings, and whether logging is enabled, use the **show ip dns view** command in privileged EXEC mode.

show ip dns view [**vrf** *vrf-name*] [**default** | *view-name*]

Syntax Description

vrf *vrf-name*	(Optional) The *vrf-name* argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view. Default is the global VRF (that is, the VRF whose name is a NULL string). **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
default	(Optional) Specifies that the DNS view is unnamed. By default all configured DNS views are displayed.
view-name	(Optional) Name of the DNS view whose information is to be displayed. Default is all configured DNS views. **Note** More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Display DNS view information to view its DNS resolver settings, DNS forwarder settings, and whether logging is enabled.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Because different DNS views can be associated with the same VRF, omitting both the **default** keyword and the *view-name* argument causes this command to display information about all the views associated with the global or named VRF.

Command Examples

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

```
Router# show ip dns view

DNS View default parameters:
Logging is on (view used 102 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example.com
  Domain search list: example1.com example2.com example3.com
  Domain name for multicast lookups: 192.0.2.10
  Lookup timeout: 7 seconds
  Lookup retries: 5
  Domain name-servers:
    192.168.2.204
    192.168.2.205
    192.168.2.206
  Round-robin'ing of IP addresses is enabled
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.11
    192.168.2.12
    192.168.2.13
  Forwarder source interface: FastEthernet0/1
DNS View user5 parameters:
Logging is on (view used 10 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example5.net
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    192.168.2.104
    192.168.2.105
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.204
DNS View user1 vrf vpn101 parameters:
Logging is on (view used 7 times)
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: example1.com
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    192.168.2.100
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
    192.168.2.200 (vrf vpn201)
```

The table below describes the significant fields shown for each DNS view in the display.

Table 19: show ip dns view Field Descriptions

Field	Description
Logging	Logging of a system message logging (syslog) message each time the DNS view is used. Configured using the **logging** command. **Note** If logging is enabled for a DNS view, the **show ip dns view** command output includes the number of times the DNS view has been used in responding to DNS queries.
Domain lookup	DNS lookup to resolve hostnames for internally generated queries. Enabled or disabled using the **domain lookup** command.
Default domain name	Default domain to append to hostnames without a dot. Configured using the **domain name** command.
Domain search list	List of domain names to try for hostnames without a dot. Configured using the **domain list** command.
Domain name for multicast lookups	IP address to use for multicast address lookups. Configured using the **domain multicast** command.
Lookup timeout	Time (in seconds) to wait for DNS response after sending or forwarding a query. Configured using the **domain timeout** command.
Lookup retries	Number of retries when sending or forwarding a query. Configured using the **domain retry** command.
Domain name-servers	Up to six name servers to use to resolve domain names for internally generated queries. Configured using the **domain name-server** command.
Resolver source interface	Source interface to use to resolve domain names for internally generated queries. Configured using the **ip domain lookup source-interfac**e global command.
Round robin'ing of IP addresses	Round-robin rotation of the IP addresses associated with the hostname in cache each time hostnames are looked up. Enabled or disabled using the **domain round-robin** command.
Forwarding of queries	Forwarding of incoming DNS queries. Enabled or disabled using the **dns forwarding** command.
Forwarder addresses	Up to six IP address to use to forward incoming DNS queries. Configured using the **dns forwarder** command.

Field	Description
Forwarder source-interface	Source interface to use to forward incoming DNS queries. Configured using the **dns forwarding source-interface** command.

show ip dns view-list

To display information about a Domain Name System (DNS) view list or about all configured DNS view lists, use the **show ip dns view-list** command in privileged EXEC mode.

show ip dns view-list [*view-list-name*]

Syntax Description

view-list-name	(Optional) Name of the DNS view list. Default is all configured DNS view lists.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

IP DNS view lists are defined by using the **ip dns view-list** command.

To display information about how DNS view lists are applied, use the **show running-config** command:

- The default DNS view list, if configured, is listed in the default DNS view information (in the **ip dns view default** command information, as the argument for the **ip dns server view-group** command).
- Any DNS view lists attached to interfaces are listed in the information for each individual interface (in the **interface** command information for that interface, as the argument for the **ip dns view-group** command).

Command Examples

The following is sample output from the **show ip dns view-list** command:

```
Router# show ip dns view-list

View-list userlist1:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to source ACL: 71
    Restrict to ip dns name-list: 151
  View user3 vrf vpn103:
    Evaluation order: 30
    Restrict to source ACL: 71
```

```
    Restrict to ip dns name-list: 151
View-list userlist2:
  View user1 vrf vpn101:
    Evaluation order: 10
    Restrict to ip dns name-list: 151
  View user2 vrf vpn102:
    Evaluation order: 20
    Restrict to ip dns name-list: 151
  View user3 vrf vpn103:
    Evaluation order: 30
    Restrict to ip dns name-list: 151
```

The table below describes the significant fields shown for each DNS view list in the display.

Table 20: show ip dns view-list Field Descriptions

Field	Description
View-list	A DNS view list name. Configured using the **ip dns view** command.
View	A DNS view that is a member of this DNS view list. If the view is associated with a VRF, the VRF name is also displayed. Configured using the **ip dns view-list** command.
Evaluation order	Indication of the order in which the DNS view is checked, relative to other DNS views in the same DNS view list. Configured using the **view** command.
Restrict	Usage restrictions for the DNS view when it is a member of this DNS view list. Configured using the **restrict name-group** command or the **restrict source access-group** command.

Related Commands

Command	Description
debug ip dns view-list	Enables debugging output for DNS view list events.
interface	Configures an interface type and enter interface configuration mode so that the specific interface can be configured.
ip dns server view-group	Specifies the DNS view list to use to determine which DNS view to use handle incoming queries that arrive on an interface not configured with a DNS view list.
ip dns view-group	Specifies the DNS view list to use to determine which DNS view to use to handle incoming DNS queries that arrive on a specific interface.

Command	Description
ip dns view-list	Enters DNS view list configuration mode so that DNS views can be added to or removed from the ordered list of DNS views.
show running-config	Displays the contents of the currently running configuration file of your routing device.

show ip host-list

To display the assigned hosts in a list, use the **show ip host-list** command in privileged EXEC mode.

show ip host-list [*host-list-name*]

Syntax Description

host-list-name	(Optional) Name assigned to the list of hosts.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Command Examples

The following is sample output from the **show ip host-list** command example for the abctest group:

```
Router# show ip host-list abctest
Host list: abctest
 ddns.abc.test
 10.2.3.4
 ddns2.unit.test
 10.3.4.5
 ddns3.com
 10.3.3.3
 e.org
 1.org.2.org
 3.com
 10.5.5.5 (VRF: def)
```

Related Commands

Command	Description
debug dhcp	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
debug ip ddns update	Enables debugging for DDNS updates.
debug ip dhcp server	Enables DHCP server debugging.
host (host-list)	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.

Command	Description
ip ddns update hostname	Enables a host to be used for DDNS updates of A and PTR RRs.
ip ddns update method	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.
ip dhcp client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp-client update dns	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
ip dhcp update dns	Enables DDNS updates of A and PTR RRs for most address pools.
ip host-list	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
show ip ddns update	Displays information about the DDNS updates.
show ip ddns update method	Displays information about the DDNS update method.
update dns	Dynamically updates a DNS with A and PTR RRs for some address pools.

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

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The command output was modified to show the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multiprocessor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.

Release	Modification
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it 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 lets the software 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, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

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.

You can use the **show ip interface brief** command to display a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Command Examples

The following example shows configuration information for interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route map named PBRNAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both Policy Based Routing (PBR) and NetFlow features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 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 unreachables 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
     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 instance. In the example, “Downstream VPN Routing/Forwarding “D”” identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 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 unreachables 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
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  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 unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No 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
  Probe proxy name replies are 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
```

Examples

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  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 unreachables 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 Fast switching turbo vector
  IP Normal 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
  Probe proxy name replies are 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
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

The table below describes the significant fields shown in the display.

Table 21: show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.

Field	Description
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
Downstream VPN Routing/Forwarding “D”	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays “Flow init” to specify that NetFlow is enabled on the interface. Displays “Ingress Flow”

Field	Description
	to specify that NetFlow is enabled on a subinterface using the **ip flow ingress**command. Shows “Flow” to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays “enabled” or “disabled.”
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays “enabled” or “disabled.”
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The following example shows how to display a summary of the usability status information for each interface:

```
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
```

The table below describes the significant fields shown in the display.

Table 22: 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 valid. “No” means that the IP Address is not valid.
Method	The Method field has the following possible values:

Field	Description
	• RARP or SLARP--Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP--Bootstrap protocol. • TFTP--Configuration file obtained from the TFTP server. • manual--Manually changed by the command-line interface. • NVRAM--Configuration file in NVRAM. • IPCP--**ip address negotiated** command. • DHCP--**ip address dhcp** command. • unassigned--No IP address. • unset--Unset. • other--Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up--Interface is up. • down--Interface is down. • administratively down--Interface is administratively down.
Protocol	Shows 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.

Command	Description
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** command in EXEC mode.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Command 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.