match reply prefix-list through utilization mark low

match reply prefix-list

To enable verification of the advertised prefixes in the Dynamic Host Configuration Protocol (DHCP) reply messages from the configured authorized prefix list, use the **match reply prefix-list** command in DHCPv6 guard configuration mode. To disable verification of the advertised prefixes in the DHCP reply messages from the configured authorized prefix list, use the **no** form of this command.

match reply prefix-list *ipv6 prefix-list name*

no match reply prefix-list *ipv6 prefix-list name*

Syntax Description

ipv6 prefix-list name	The name of the prefix list.

Command Default

The advertised prefixes in DHCP reply messages from the configured authorized prefix list are not verified.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. A prefix list is configured using the **ipv6 prefix-list** command. An empty prefix list is treated as a permit.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# match reply prefix-list ipv6pre1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.

match server access-list

To enable verification of the advertised Dynamic Host Configuration Protocol (DHCP) server or relay address in inspected messages from the configured authorized server access list, use the **match server access-list** command in DHCPv6 guard configuration mode. To disable verification of the advertised DHCP server or relay address in inspected messages from the configured authorized server access list, use the **no** form of this command.

match server access-list *ipv6 access-list-name*

no match server access-list *ipv6 access-list-name*

Syntax Description

ipv6 access-list-name	The name of the access list.

Command Default

The advertised DHCP server or relay address in inspected messages from the configured authorized server access list are not verified.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

Enables verification of the advertised DHCP server or relay address in inspected messages from the configured authorized server access list. If not configured, this check will be bypassed. An access list is configured using the **ipv6 access-list** command. An empty access list is treated as a permit. The access list is configured using the **ipv6 access-list** command.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification of the advertised DHCP server or relay address in inspected messages from the configured authorized server access list:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# match server access-list ipv6acl1
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.
ipv6 access-list	Defines an IPv6 access list.

netbios-name-server

To configure NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-name-server** command in DHCP pool configuration. To remove the NetBIOS name server list, use the no form of this command.

netbios-name-server *address* [*address2 ... address8*]

no netbios-name-server

Syntax Description

address	Specifies the IP address of the NetBIOS WINS name server. One IP address is required, although you can specify up to eight addresses in one command line.
address2 ...address8	(Optional) Specifies up to eight addresses in the command line.

Command Modes

DHCP pool configuration

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.

Usage Guidelines

One IP address is required, although you can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies the IP address of a NetBIOS name server available to the client:

```
netbios-name-server 10.12.1.90
```

Related Commands

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.

Command	Description
domain-name (DHCP)	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios-node-type	Configures the NetBIOS node type for Microsoft DHCP clients.

netbios-node-type

To configure the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients, use the **netbios-node-type** command in DHCP pool configuration mode. To remove the NetBIOS node type, use the no form of this command.

netbios-node-type *type*

no netbios-node-type

Syntax Description

type	Specifies the NetBIOS node type. Valid types are: • **b-node** --Broadcast • **p-node** --Peer-to-peer • **m-node** --Mixed • **h-node** --Hybrid (recommended)

Command Modes

DHCP pool configuration

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.

Usage Guidelines

The recommended type is h-node (hybrid).

Examples

The following example specifies the client's NetBIOS type as hybrid:

```
netbios node-type h-node
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
netbios name-server	Configures NetBIOS WINS name servers that are available to Microsoft DHCP clients.

network (DHCP)

To configure the network number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool primary or secondary subnet on a Cisco IOS DHCP server, use the **network** command in DHCP pool configuration mode. To remove the subnet number and mask, use the **no** form of this command.

[1]

[2]

Syntax Description

network-number	The IP address of the primary DHCP address pool.
mask	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.
/ *prefix-length*	(Optional) The number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
secondary	(Optional) The network address specifies a secondary subnet in the DHCP address pool, and the router enters DHCP pool secondary subnet configuration mode. **Note** To configure a secondary subnet, you must also specify the *mask* argument or the p*refix-length* argument.

Command Default

This command is disabled by default.

Command Modes

DHCP pool configuration (dhcp-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.
12.2(33)SRB	This command was modified. The **secondary** keyword was added.

[1]

[2]

Release	Modification
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 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

This command is valid for DHCP subnetwork address pools only.

The DHCP server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the **ip dhcp excluded-address** global configuration command. However, the **ip dhcp excluded-address** command cannot be used to exclude addresses from virtual routing and forwarding (VRF)-associated pools.

You cannot configure manual bindings within the same pool that is configured with the **network** command.

If a default router list is configured for the pool or subnet from which the address was allocated, the DHCP server selects an IP address from that default router list and provides it to the client. The DHCP client uses that router as the first hop for forwarding messages.

Removing a secondary subnet also removes the default router list for that subnet. Removing the primary subnet removes only the primary subnet definition but not the network-wide default router list.

To display the DHCP address pool information configured by the **network** command, use the **show ip dhcp pool** command.

Examples

The following example shows how to configure 172.16.0.0/12 as the subnetwork number and mask of the DHCP pool named pool1. The IP addresses in pool1 range from 172.16.0.0 to 172.31.255.255.

```
Router(config)#
ip dhcp pool pool1

Router(dhcp-config)#
network 172.16.0.0 255.240.0.0
```

The following example shows how to configure 192.0.2.0/24 as the subnetwork number and mask of the DHCP pool named pool2 and then add the DHCP pool secondary subnet specified by the subnet number and mask 192.0.4.0/30. The IP addresses in pool2 consist of two unconnected subnets: the addresses from 192.0.2.1 to 192.0.2.254 and the addresses from 192.0.4.1 to 192.0.4.2.

```
Router(config)#
ip dhcp pool pool2

Router(dhcp-config)#
network 192.0.2.0 255.255.255.0

Router(dhcp-config)#
network 192.0.4.0 255.255.255.252 secondary
```

Related Commands

Command	Description
default-router	Specifies the IP address of the default router for a DHCP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
override default-router	Configures a subnet-specific default router list for the DHCP pool secondary subnet.
show ip dhcp pool	Displays information about the DHCP address pools.

next-server

To configure the next server in the boot process of a Dynamic Host Configuration Protocol (DHCP) client, use the **next-server** command in DHCP pool configuration. To remove the boot server list, use the **no** form of this command.

next-server *address* [*address2 ... address8*]

no next-server *address*

Syntax Description

address	Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server. One IP address is required, but up to eight addresses can be specified in one command line.
address2 ...address8	(Optional) Specifies up to seven additional addresses in the command line.

Command Default

If the **next-server** command is not used to configure a boot server list, the DHCP Server uses inbound interface helper addresses as boot servers.

Command Modes

DHCP pool configuration

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.

Usage Guidelines

You can specify up to eight servers in the list. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the next server in the boot process:

```
next-server 10.12.1.99
```

Related Commands

Command	Description
accounting (DHCP)	Specifies the name of the default boot image for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip helper-address	Forwards UDP broadcasts, including BOOTP, received on an interface.
option	Configures Cisco IOS DHCP server options.

option

To configure DHCP server options, use the **option** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

option *code* [**instance** *number*] {**ascii** *string*| **hex** {*string*| **none**}| **ip** {*address*| *hostname*}}

no option *code* [**instance** *number*]

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254.
instance *number*	(Optional) Specifies an instance number. The range is from 0 to 255. The default is 0.
ascii *string*	Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white spaces must be delimited by quotation marks. The ASCII value is truncated to 255 characters entered.
hex	Specifies dotted hexadecimal data.
string	Hexadecimal value truncated to 180 characters entered. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period, colon, or white space.
none	Specifies the zero-length hexadecimal string.
ip *address*	Specifies an IP address. More than one IP address can be specified.
ip *hostname*	Specifies the hostname. More than one hostname can be specified.

Command Default

The default instance number is 0.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was 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(24)T	This command was modified. The **none** keyword was added.
15.1(3)S	This command was modified. A maximum limit of 180 characters was set for the dotted hexadecimal data and 255 characters for the ASCII data.

Usage Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. The configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options is documented in RFC 2131, *Dynamic Host Configuration Protocol*.

Examples

The following example shows how to configure DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding; a value of 1 means enable IP forwarding. IP forwarding is enabled in the following example.

```
Router(config)# ip dhcp pool red
Router(dhcp-config)# option 19 hex 01
```

The following example shows how to configure DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example.

```
Router(config)# ip dhcp pool red
Router(dhcp-config)# option 72 ip 172.16.3.252 172.16.3.253
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

origin

To configure an address pool as an on-demand address pool (ODAP) or static mapping pool, use the **origin** command in DHCP pool configuration mode. To disable the ODAP, use the **no** form of this command.

origin {**dhcp** [**number** *number*| **subnet size initial** *size* [**autogrow** *size*]]| **aaa** [**subnet size initial** *size* [**autogrow** *size*]]| **file** *url* [**refresh** [**interval** *minutes*]]| **ipcp**}

no origin {**dhcp** [**number** *number*| **subnet size initial** *size* [**autogrow** *size*]]| **aaa** [**subnet size initial** *size* [**autogrow** *size*]]| **file** *url* [**refresh** [**interval** *minutes*]]| **ipcp**}

Syntax Description

dhcp	Specifies Dynamic Host Configuration Protocol (DHCP) as the subnet allocation protocol.
number *number*	(Optional) Specifies the number of subnets to request. The range is from 1 to 5.
subnet size initial *size*	(Optional) Specifies the initial size of the first requested subnet. You can enter the value for the *size* argument as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.
autogrow *size*	(Optional) Specifies that the pool can grow incrementally. The value for the *size* argument is the size of the requested subnets when the pool requests additional subnets (upon detection of high utilization). You can enter the value for the *size* as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.
aaa	Specifies authentication, authorization, and accounting (AAA) as the subnet allocation protocol.
file *url*	Specifies the external database file that contains the static bindings assigned by the DHCP server. The *url* argument specifies the location of the external database file.
refresh	Specifies to refresh or reread the DHCP static mapping file.
interval *minutes*	Specifies the refresh or reread interval, in minutes, for DHCP static mapping file. The range is from 1 to 500.
ipcp	Specifies the IP Control Protocol (IPCP) as the subnet allocation protocol.

Command Default

The default value for the *size* argument is /0.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(11)T	This command was modified. The **file** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
15.2(1)T	This command was modified. The **number**, **refresh**, and **interval** keywords and the *number* and *minutes* arguments were added.

Usage Guidelines

If you do not configure the pool as an autogrow pool, the pool will not request additional subnets if one subnet is already in the pool.

Use the **dhcp** keyword to obtain subnets from DHCP, the **aaa** keyword to obtain subnets from the AAA server, and the **ipcp** keyword to obtain subnets from IPCP negotiation. If you expect that the utilization of the pool may grow over time, use the **autogrow** *size* option.

If a pool has been configured with the **autogrow** *size* option, ensure that the source server can provide more than one subnet to the same pool. Even though the Cisco IOS software specifies the requested subnet size, it can accept any offered subnet size from the source server.

Examples

The following example shows how to configure an address pool named pool1 to use DHCP as the subnet allocation protocol with an initial subnet size of 24 and an autogrow subnet size of 24:

```
ip dhcp pool pool1
  vrf pool1
  origin dhcp subnet size initial /24 autogrow /24
  utilization mark high 80
  utilization mark low 20
```

The following example shows how to configure the location of the external text file:

```
ip dhcp pool abcpool
 origin file tftp://10.1.0.1/staticbindingfile
```

Related Commands

Command	Description
show ip dhcp pool	Displays information about the DHCP address pools.

override default-router

To define a default router list for the DHCP pool secondary subnet, use the **override default-router** command in DHCP pool secondary subnet configuration mode. To remove the default router list for this secondary subnet, use the **no** form of this command.

override default-router *address* [*address2 ... address8*]

no override default-router

Syntax Description

address	IP address of the default router for the DHCP pool secondary subnet, preferably on the same subnet as the DHCP pool secondary client subnet.
address2 ... address8	(Optional) IP addresses of up to seven additional default routers, delimited by a single space. **Note** The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering IP addresses.

Command Default

No default router list is defined for the DHCP pool secondary subnet.

Command Modes

DHCP pool secondary subnet configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

When an IP address is assigned to the DHCP client from a secondary subnet for which no subnet-specific default router list is defined, the default router list (configured by using the **default-router** command in DHCP pool configuration mode) will be used.

The IP address of every router in the list should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (*address* is the most preferred router, *address2* is the next most preferred router, and so on).

To display the default router lists, use the **show running-config** command. If default router lists are configured for a DHCP pool, the commands used to configure those lists are displayed following the **ip dhcp pool** command that configures the DHCP pool.

Examples

The following example configures 10.1.1.1/29 as the subnetwork number and mask of the DHCP pool named pool1, adds the DHCP pool secondary subnet specified by the subnet number and mask 10.1.1.17/29, then configures a subnet-specific default router list for that subnet:

```
Router(config)# dhcp pool pool1

Router(config-dhcp)# network 10.1.1.1 255.255.255.248

Router(config-dhcp)# network 10.1.1.17 255.255.255.248 secondary

Router(config-dhcp-secondary-subnet)# override default-router 10.1.1.100 10.1.1.200
```

Related Commands

Command	Description
default-router	Specifies the default router list for a DHCP client.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server.

override utilization high

To configure the high utilization mark of the current secondary subnet size, use the **override utilization high** command in DHCP pool secondary subnet configuration mode. To remove the high utilization mark, use the **no** form of this command.

override utilization high *percentage-number*

no override utilization high *percentage-number*

Syntax Description

percentage-number	Percentage of the current subnet size. The range is from 1 to 100 percent.

Command Default

The default high utilization mark is 100 percent of the current subnet size.

Command Modes

DHCP pool secondary subnet configuration (config-dhcp-subnet-secondary)

Command History

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

Usage Guidelines

If you use the **utilization mark** {**high** | **low**} **log** command, a system message can be generated for a DHCP secondary subnet when the subnet utilization exceeds the configured high utilization threshold. A system message can also be generated when the subnet's utilization is detected to be below the configured low utilization threshold.

The **override utilization high** command overrides the value specified by the **utilization mark high** global configuration command.

Examples

The following example shows how to set the high utilization mark of the secondary subnet to 40 percent of the current subnet size:

```
Router(config)# ip dhcp pool pool2
Router(dhcp-config)# utilization mark high 80 log
Router(dhcp-config)# utilization mark low 70 log
Router(dhcp-config)# network 192.0.2.0 255.255.255.0
Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary
Router(config-dhcp-subnet-secondary)# override utilization high 40
Router(config-dhcp-subnet-secondary)# override utilization low 30
```

Related Commands

Command	Descriptions
override utilization low	Configures the low utilization mark of the current subnet size.
utilization mark high	Configures the high utilization mark of the current address pool size.

override utilization low

To configure the low utilization mark of the current secondary subnet size, use the **override utilization low** command in DHCP pool secondary subnet configuration mode. To remove the low utilization mark, use the **no** form of this command.

override utilization low *percentage-number*

no override utilization low *percentage-number*

Syntax Description

percentage-number	Percentage of the current subnet size. The range is from 1 to 100.

Command Default

The default low utilization mark is 0 percent of the current subnet size.

Command Modes

DHCP pool secondary subnet configuration (config-dhcp-subnet-secondary)

Command History

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

Usage Guidelines

If you use the **utilization mark**{**high**| **low**} **log** command, a system message can be generated for a DHCP secondary subnet when the subnet utilization falls below the configured low utilization threshold. A system message can also be generated when the subnet's utilization exceeds the configured high utilization threshold.

The **override utilization low** command overrides the value specified by the **utilization mark low** global configuration command.

Examples

The following example shows how to set the low utilization mark of the secondary subnet to 30 percent of the current subnet size:

```
Router(config)# ip dhcp pool pool2

Router(dhcp-config)# utilization mark high 80 log

Router(dhcp-config)# utilization mark low 70 log

Router(dhcp-config)# network 192.0.2.0 255.255.255.0

Router(dhcp-config)# network 192.0.4.0 255.255.255.252 secondary

Router(config-dhcp-subnet-secondary)# override utilization high 40

Router(config-dhcp-subnet-secondary)# override utilization low 30
```

Related Commands

Command	Description
override utilization high	Configures the high utilization mark of the current subnet size.
utilization mark low	Configures the low utilization mark of the current address pool size.

preference (DHCPv6 Guard)

To enable verification that the advertised preference (in preference option) is greater than the minimum specified limit and less than the maximum specified limit, use the **preference** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To remove the preference, use the **no** form of this command.

preference{**max**| **min**}*limit*

no preference{**max**| **min**}*limit*

Syntax Description

limit	The maximum or minimum limit that the advertised preference must conform to. The acceptable range is from 0 to 255.

Command Default

No preference value is set.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command enables verification that the advertised preference is not greater than the maximum specified limit or less than the minimum specified limit.

Examples

The following example defines an DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification that the advertised preference is not greater than 254 or less than 2:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# preference min 2
Router(config-dhcp-guard)# preference max 254
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

relay agent information

To enter relay agent information option configuration mode, use the **relay agent information**command in DHCP class configuration mode. To disable this functionality, use the **no** form of this command.

relay agent information

no relay agent information

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

DHCP class configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

If this command is omitted for Dynamic Host Configuration Protocol (DHCP) class-based address allocation, then the DHCP class matches to any relay agent information option, whether it is present or not.

Using the **no relay agent information** command removes all patterns in the DHCP class configured by the **relay-information hex** command.

Examples

The following example shows the relay information patterns configured for DHCP class 1.

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF
ip dhcp class CLASS2
 relay agent information
```

Related Commands

Command	Description
relay-information hex	Specifies a hexadecimal string for the full relay agent information option.

relay-information hex

To specify a hexadecimal string for the full relay agent information option, use the **relay-information hex** command in relay agent information option configuration mode. To remove the configuration, use the **no** form of this command.

relay-information hex *pattern* **[*]** [**bitmask** *mask*]

no relay-information hex *pattern* **[*]** [**bitmask** *mask*]

Syntax Description

pattern	String of hexadecimal values. This string creates a pattern that is matched against the named DHCP class.
*	(Optional) Wildcard character.
bitmask *mask*	(Optional) Hexadecimal bitmask.

Command Default

No default behavior or values

Command Modes

Relay agent information option configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **relay-information hex** command sets a pattern that is used to match against defined DHCP classes. You can configure multiple **relay-information hex** commands for a DHCP class. This is useful to specify a set of relay information options that can not be summarized with a wildcard or a bitmask.

The pattern itself, excluding the wildcard, must contain a whole number of bytes (a byte is two hexadecimal numbers). For example, 010203 is 3 bytes (accepted) and 01020 is 2.5 bytes (not accepted).

If you omit this command, no pattern is configured and it is considered a match to any relay agent information value, but the relay information option must be present in the DHCP packet.

You must know the hexadecimal value of each byte location in option 82 to be able to configure the **relay-information hex** command. The option 82 format may vary from product to product. Contact the relay agent vendor for this information.

Examples

The following example shows the configured relay agent information patterns. Note that CLASS 2 has no pattern configured and will “match to any” class.

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF
ip dhcp class CLASS2
 relay agent information
```

remote-span

To configure a virtual local area network (VLAN) as a remote switched port analyzer (RSPAN) VLAN, use the **remote-span** command in config-VLAN mode. To remove the RSPAN designation, use the **no** form of this command.

remote-span

no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

Release	Modification
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 Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Cisco 7600 series router.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands

Connect	Description
show vlan remote-span	Displays a list of RSPAN VLANs.

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).

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.

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.

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.

Command	Description
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 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.

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 2: 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.

Field	Description
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.
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 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.

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 3: 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 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.

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 : 020a00001400006400000000
```

Table 4: 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 5: 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.

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 6: 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.

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 7: 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.

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 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.

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 8: 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 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.

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 9: 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.

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.
ip dhcp snooping database	Configures the DHCP-snooping database.
ip dhcp snooping information option	Enables DHCP option 82 data insertion.

Command	Description
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.

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 10: 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.

Command	Description
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.

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 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.
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.

Release	Modification
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.

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 11: 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.
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.

Field	Description
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" 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.

Field	Description
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 12: 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.

Field	Description
Method	The Method field has the following possible values: • 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. • 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.

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ip route dhcp

To display the routes added to the routing table by the Dynamic Host Configuration Protocol (DHCP) server and relay agent, use the **show ip route dhcp** command in privileged EXEC configuration mode.

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

Syntax Description

vrf	(Optional) Specifies VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name of the VRF.
ip-address	(Optional) Address about which routing information should be displayed.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	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

To display information about global routes, use the **show ip route dhcp** command. To display routes in the VRF routing table, use the **show ip route vrf** *vrf-name* **dhcp** command.

Examples

The following is sample output from the **show ip route dhcp**command when entered without an address. This command lists all routes added by the DHCP server and relay agent.

```
Router# show ip route dhcp
  10.5.5.56/32 is directly connected, ATM0.2
  10.5.5.217/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route dhcp** command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route dhcp 10.5.5.217

  10.5.5.217 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 01:19 PM
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp**command when entered without an address:

```
Router# show ip route vrf abc dhcp
  10.5.5.218/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route vrf** *vrf-name* **dhcp**command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route vrf red dhcp 10.5.5.218
  10.5.5.218/32 is directly connected, ATM0.2
    DHCP Server: 10.9.9.10   Lease expires at Nov 08 2001 03:15PM
```

Related Commands

Command	Description
clear ip route dhcp	Removes routes from the routing table added by the DHCP server and relay agent for the DHCP clients on unnumbered interfaces.

show ip source binding

To display IP-source bindings configured on the system, use the **show ip source command** command in privileged EXEC mode.

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping| static**] [**vlan** *vlan-id*] [**interface** *type mod/port*]

Syntax Description

ip-address	(Optional) Binding IP address.
mac-address	(Optional) Binding MAC address.
dhcp-snooping	(Optional) Specifies DHCP snooping binding entry.
static	(Optional) Specifies a static binding entry.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
interface *type*	(Optional) Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number.

Command Default

Both static and DHCP-snooping bindings are displayed.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Each optional parameter is used to filter the display output.

Examples

This example shows the output without entering any keywords:

Router# **show ip source binding**

```
MacAddress             IpAddress       Lease(sec) Type          VLAN Interface
------------------     --------------- ---------- ------------- ---- --------------------
```

```
00:00:00:0A:00:0B      17.16.0.1        infinite   static        10   FastEthernet6/10
00:00:00:0A:00:0A      17.16.0.2        10000      dhcp-snooping 10   FastEthernet6/11
```

This example shows how to display the static IP binding entry for a specific IP address:

```
Router# show ip source binding 17.16.0.1 0000.000A.000B static vlan 10 interface
gigabitethernet6/10
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------

00:00:00:0A:00:0B   17.16.0.1         infinite    static         10    FastEthernet6/10
```

The table below describes the significant fields in the display.

Table 13: show ip source binding Field Descriptions

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; static bindings configured from CLI to dynamic binding learned from DHCP snooping.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per 12-port IP source guard.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

show ip verify source

To display the IP source guard configuration and filters on a particular interface, use the **show ip verify source** command in EXEC mode.

show ip verify source [**interface** *type mod*/*port*] [**efp_id efp_id**]

Syntax Description

interface *type*	(Optional) Specifies the interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod / *port*	Module and port number.
efp_id	(Optional) Specifies the Ethernet flow point (EFP) (service instance) ID.
efp_id	EFP number; range is 1 to 8000.

Command Default

This command has no default settings.

Command Modes

EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRD	The **efp_id** *efp_id*keyword and argument were added.

Usage Guidelines

Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

Examples

This example shows the display when DHCP snooping is enabled on VLANs 10 to 20, the interface has IP source filter mode that is configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

```
Router# show ip verify source interface gigabitethernet6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                       11-20
```

This example shows how to display the IP source guard configuration and filters on a specific interface:

```
Router# show ip verify source interface gigabitethernet6/1
```

```
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           inactive-trust-port
```

This example shows the display when the interface does not have a VLAN enabled for DHCP snooping:

```
Router# show ip verify source interface gigabitethernet6/3
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/3      ip           inactive-no-snooping-vlan
```

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 10.0.0.1/aaaa.bbbb.cccd on VLAN 11:

```
Router# show ip verify source interface gigabitethernet6/4
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi6/4      ip-mac       active       10.0.0.1         aaaa.bbbb.cccd  11
gi6/4      ip-mac       active       deny-all         deny-all        12-20
```

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binding 10.0.0.3/aaaa.bbbb.ccce on VLAN 10, but port security is not enabled on the interface:

```
Router# show ip verify source interface gigabitethernet6/5
Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
```

This example shows the display when the interface does not have IP source filter mode configured:

```
Router# show ip verify source interface gigabitethernet6/6
DHCP security is not configured on the interface gi6/6.
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source

Interface  Filter-type  Filter-mode  IP-address       Mac-address     Vlan
---------  -----------  -----------  ---------------  --------------  ---------
gi6/1      ip           active       10.0.0.1                         10
gi6/1      ip           active       deny-all                         11-20
gi6/2      ip           inactive-trust-port
gi6/3      ip           inactive-no-snooping-vlan
gi6/4      ip-mac       active       10.0.0.2         aaaa.bbbb.cccc  10
gi6/4      ip-mac       active       11.0.0.1         aaaa.bbbb.cccd  11
gi6/4      ip-mac       active       deny-all         deny-all        12-20
gi6/5      ip-mac       active       10.0.0.3         permit-all      10
gi6/5      ip-mac       active       deny-all         permit-all      11-20
Router#
```

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source interface gi5/0/0 efp_id 10
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan        EFP
ID
---------    -----------    -----------      ---------------     -----------------
----------  ----------
Gi5/0/0    ip-mac       active          123.1.1.1        00:0A:00:0A:00:0A  100        10

Gi5/0/0    ip-mac       active          123.1.1.2        00:0A:00:0A:00:0B  100        20

Gi5/0/0    ip-mac       active          123.1.1.3        00:0A:00:0A:00:0C  100        30
```

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per l2-port IP source guard.
show ip source binding	Displays the IP-source bindings configured on the system.

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

show ipv6 dhcp conflict [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	(Optional) The address of a DHCP for IPv6 client.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(2)S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.3S	This command was modified. The **vrf** *vrf-name* keyword and argument were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
     2001:0DB8:1005::10
```

Related Commands

Command	Description
clear ipv6 dhcp conflict	Clears an address conflict from the DHCPv6 server database.

trusted-port (DHCPv6 Guard)

To configure a port to become a trusted port, use the **trusted-port** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, messages received on ports that have this policy are not verified.

Examples

The following example defines a DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and sets the port to trusted:

```
Router(config)# ipv6 dhcp guard policy policy1
Router(config-dhcp-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

utilization mark high

To configure the high utilization mark of the current address pool size, use the **utilization mark high** command in DHCP pool configuration mode. To remove the high utilization mark, use the **no** form of this command.

utilization mark high *percentage-number* **[log]**

no utilization mark high *percentage-number* **[log]**

Syntax Description

percentage-number	Percentage of the current pool size.
log	(Optional) Enables the logging of a system message.

Command Default

The default high utilization mark is 100 percent of the current pool size.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(4)T	The **log** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level exceeds the configured high utilization mark, the pool will schedule a subnet request.

This command can be used with both network and on-demand pools. However, in the case of a network pool, only the **log** option of this command can be used. In the case of an on-demand pool, the **autogrow** *size*option of the **origin** command must be configured.

In certain network deployments, it is important for the network administrator to receive asynchronous notification when the DHCP pools are nearly exhausted so that preventive action can be taken. One common method for such notification is the generation of a system message.

If you use the **log** option, a system message can be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold. A system message can also be generated when the pool's utilization is detected to be below the configured low utilization threshold.

Examples

The following example sets the high utilization mark to 80 percent of the current pool size:

```
utilization mark high 80
```

The following pool configuration using the **log** keyword option generates a system message:

```
! ip dhcp pool abc
utilization mark high 30 log
utilization mark low 25 log
network 10.1.1.0 255.255.255.248
!
```

The following system message is generated when the second IP address is allocated from the pool:

```
00:02:01: %DHCPD-6-HIGH_UTIL: Pool "abc" is in high utilization state (2 addresses used out
 of 6). Threshold set at 30%.
```

The following system message is generated when one of the two allocated IP addresses is returned to the pool:

```
00:02:58: %DHCPD-6-LOW_UTIL: Pool "abc" is in low utilization state (1 addresses used out
of 6). Threshold set at 25%.
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark low	Configures the low utilization mark of the current address pool size.

utilization mark low

To configure the low utilization mark of the current address pool size, use the **utilization mark low** command in DHCP pool configuration mode. To remove the low utilization mark, use the **no** form of this command.

utilization mark low *percentage-number*

no utilization mark low *percentage-number*

Syntax Description

percentage-number	Percentage of the current pool size.

Command Default

The default low utilization mark is 0 percent of the current pool size.

Command Modes

DHCP pool configuration

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.

Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level drops below the configured low utilization mark, a subnet release is scheduled from the address pool.

This command can be used with both network and on-demand pools. However, in the case of a network pool, only the **log** option of this command can be used. In the case of an on-demand pool, the **autogrow** *size*option of the **origin** command must be configured.

In certain network deployments, it is important for the network administrator to receive asynchronous notification when the DHCP pools are nearly exhausted so that preventive action can be taken. One common method for such notification is the generation of a system message.

If you use the **log** option, a system message can be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold. A system message can also be generated when the pool's utilization is detected to be below the configured low utilization threshold.

Examples

The following example sets the low utilization mark to 20 percent of the current pool size:

```
utilization mark low 20
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.
utilization mark high	Configures the high utilization mark of the current address pool size.