

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 mode. 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

<i>address</i>	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.
<i>address2...address8</i>	(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.
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

<i>type</i>	Specifies the NetBIOS node type. Valid types are: <ul style="list-style-type: none"> • 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.

```
network network-number [mask secondary] | /prefix-length secondary]
```

```
no network network-number [mask secondary] | /prefix-length secondary]
```

Syntax Description

<i>network-number</i>	The IP address of the primary DHCP address pool.
<i>mask</i>	(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.
<i>/prefix-length</i>	(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 <i>mask</i> argument or the <i>prefix-length</i> argument.

Defaults

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.
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 mode. To remove the boot server list, use the **no** form of this command.

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

```
no next-server address
```

Syntax Description

<i>address</i>	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.
<i>address2...address8</i>	(Optional) Specifies up to seven additional addresses in the command line.

Defaults

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 Dynamic Host Configuration Protocol (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}
```

```
no option code [instance number]
```

Syntax Description		
<i>code</i>	Specifies the DHCP option code. The range is from 0 to 254.	
instance <i>number</i>	(Optional) Specifies an instance number. The range is from 0 to 255. The default is 0.	
ascii <i>string</i>	Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.	
hex	Specifies dotted hexadecimal data.	
<i>string</i>	Hexadecimal value. 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 <i>address</i>	Specifies the hostname or an IP address. More than one hostname or IP address can be specified with one CLI.	

Defaults

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.
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.

Usage Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. 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 are documented in RFC 2131, *Dynamic Host Configuration Protocol*.

Examples

The following example configures 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 configures 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 the DHCP pool configuration mode.

option hex

To enable the Cisco IOS relay agent to make forwarding decisions based on DHCP options inserted in the client-generated DHCP message, use the **option hex** command in DHCP class configuration mode. To disable this functionality, use the **no** form of this command.

option *code* **hex** *hex-pattern* [*] [**bit** *bit-mask-pattern*]

no option *code* **hex** *hex-pattern* [*] [**mask** *bit-mask-pattern*]

Syntax Description

<i>code</i>	Specifies the DHCP option code. Valid values are 60, 77, 124, and 125. All other values will be rejected with the appropriate error message.
<i>hex-pattern</i>	String of hexadecimal values. This string creates a pattern that is matched against the named DHCP class. The <i>hex-pattern</i> argument represents the data portion of the DHCP option format. See “Usage Guidelines” below for more information.
*	(Optional) Wildcard character.
mask <i>bit-mask-pattern</i>	(Optional) String of hexadecimal values. Specifies the bit mask to be applied to the <i>hex-pattern</i> argument.

Command Default

This command is disabled by default.

Command Modes

DHCP class configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The **option hex** command enhances DHCP class support to allow the relay agent to relay client-generated messages to different DHCP servers based on the content of the following four options:

- Option 60: vendor class identifier
- Option 77: user class
- Option 124: vendor-identifying vendor class
- Option 125: vendor-identifying vendor-specific information

Each option identifies the type of client sending the DHCP message.

[Table 16](#) describes the CLI variations possible for the **hex** *hex-pattern* keyword and argument combination.

Table 16 *option hex CLI Variations*

Hex string format variations	CLI example	Description
Full option value as raw hex	<code>option 60 hex 010203</code>	This option has 3 bytes of data with 0x010203 hex as the content.
Bit-masked hex string	<code>option 60 hex 010203 mask 0000FF</code>	This option is the same as above except that only the first 2 bytes of data should be 0x0102.
Wild-carded hex string	<code>option 60 hex 010203*</code>	This option should have at least 3 bytes, with the first 3 bytes matching the specified hex pattern.

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

Examples

In the following example, client-generated DHCP messages containing option 60 and belonging to class VOIP will be forwarded to the DHCP server located at 10.30.5.1:

```
!
ip dhcp class VOIP
 option 60 hex 010203
!
! The following is the relay pool
ip dhcp pool red
 relay source 10.2.2.0 255.255.255.0
 class VOIP
  relay target 10.30.5.1
```

Related Commands

Command	Description
ip dhcp class	Defines a DHCP class and enters DHCP class 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 | aaa | ipcp | file url } [subnet size initial size [autogrow size]]
```

```
no origin { dhcp | aaa | ipcp | file url } [subnet size initial size [autogrow size]]
```

Syntax Description

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

Defaults

The default size value is /0.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(11)T	The file keyword was added.
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.

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 is capable of providing 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 green 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
<code>show ip dhcp pool</code>	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

<i>address</i>	IP address of the default router for the DHCP pool secondary subnet, preferably on the same subnet as the DHCP pool secondary client subnet.
<i>address2 ... address8</i>	(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.

rbe nasip

To specify the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the agent remote ID option, use the **rbe nasip** command in global configuration mode. To remove the specification, use the **no** form of this command.

rbe nasip *interface-type number*

no rbe nasip

Syntax Description		
	<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default No IP address is specified.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines The **rbe nasip** command is used to configure support for the DHCP relay agent information option (option 82) for an ATM routed bridge encapsulation (RBE).

Support for the DHCP relay agent information option must be configured on the DHCP relay agent using the **ip dhcp relay information option** command for the **rbe nasip** command to be effective.

Examples The following example shows how to enable support for DHCP option 82 on the DHCP relay agent by using the **ip dhcp relay agent information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM routed bridge encapsulation is configured on ATM subinterface 4/0.1.

```
ip dhcp-server 10.1.1.1
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.5.1.1 255.255.255.0
!
interface ATM 4/0
 no ip address
```

```
!  
interface ATM 4/0.1 point-to-point  
  ip unnumbered Loopback0  
  ip helper-address 10.1.1.1  
  atm route-bridged ip  
  pvc 88/800  
    encapsulation aal5snap  
!  
router eigrp 100  
  network 10.0.0.0  
!  
rbe nasip loopback0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

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.

Defaults 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 destination

To configure an IP address for a relay destination to which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) relay agent functioning as a DHCP server, use the **relay destination** command in DHCP pool configuration mode. To disable the IP address, use the **no** form of this command.

```
relay destination [vrf vrf-name | global] ip-address
```

```
no relay destination [vrf vrf-name | global] ip-address
```

Syntax Description

vrf	(Optional) Virtual routing and forwarding (VRF) instance that is associated with the relay destination address. The <i>vrf-name</i> argument specifies the name of the VRF table.
global	(Optional) IP address selected from the global address space. If the pool does not have any VRF configuration, then the relay destination address defaults to the global address space.
<i>ip-address</i>	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Defaults

No destination IP address to which packets are forwarded is configured.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.3(14)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 integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **relay destination** command serves the same function as the **relay target** command, except that the **relay target** command specifies the DHCP server to which packets should be forwarded only for the class under which it is configured, and the **relay destination** command specifies the DHCP server to which packets should be forwarded for the pool itself. The **relay target** command overrides the **relay destination** command in cases in which the configured class name has been specified by the service gateway (SG).

When using the **relay destination** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay destination IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.

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

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

Defaults

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 01030a0b0c020500000000123
    relay-information hex 01030a0b0c02*
    relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF

ip dhcp class CLASS2
  relay agent information
```

relay source

To configure an IP address for a relay source from which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) server, use the **relay source** command in DHCP-pool configuration mode. To disable the IP address, use the **no** form of this command.

relay source *ip-address subnet-mask*

no relay source *ip-address subnet-mask*

Syntax Description		
<i>ip-address</i>		IPv4 address of DHCP server from which the DHCP client packets are relayed.
<i>subnet-mask</i>		Subnet mask that matches the subnet of the incoming interface of the DHCP client packet.

Defaults No IP address from which IP packets are forwarded is configured.

Command Modes DHCP pool configuration

Command History	Release	Modification
	12.3(14)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 integrated into Cisco IOS Release 12.2(33)SRC.

Examples The following example shows how to configure a source IP address from which DHCP client packets are relayed:

```
ip dhcp pool abc1
 relay source 10.0.0.0 255.255.0.0
 relay destination 10.5.1.1
```

Related Commands	Command	Description
	relay destination	Configures an IP address for a relay destination to which packets are forwarded by a DHCP server.
	relay target	Configures an IP address for a relay target to which packets are forward by a DHCP server.

relay target

To configure an IP address for a relay target to which packets are forwarded by a Dynamic Host Configuration Protocol (DHCP) server, use the **relay target** command in DHCP pool class configuration mode. To disable the IP address, use the **no** form of this command.

```
relay target [vrf vrf-name | global] ip-address
```

```
no relay target [vrf vrf-name | global] ip-address
```

Syntax Description

vrf	(Optional) Configured virtual routing and forwarding (VRF) that is associated with the relay destination address. The <i>vrf-name</i> argument specifies the name of the VRF table. Note If the vrf keyword is not specified, the target address is assumed to be in the same address space as the DHCP pool. If the vrf keyword is specified, the same VRF is assumed to apply here. However, if the target IP address is actually in the global address space, the global keyword should be specified.
global	(Optional) IP address selected from the global address space. If the pool does not have any VRF configuration, then the relay destination address defaults to the global address space.
<i>ip-address</i>	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Defaults

No target IP address is configured.

Command Modes

DHCP pool class configuration

Command History

Release	Modification
12.3(14)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 integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **relay target** command serves the same function as the **relay destination** command, except that the **relay target** command specifies the DHCP server to which packets should be forwarded only for the class under which it is configured, and the **relay destination** command specifies the DHCP server to which packets should be forwarded for the pool itself. The **relay target** command overrides the **relay destination** command in cases in which the configured class name has been specified by the SG.

Examples

The following example shows how to configure a relay target if a service gateway (SG)-supplied class name is used to select a DHCP server to which packets are relayed:

```
ip dhcp pool abc1
  relay source 10.0.0. 255.255.0.0.
  relay destination 10.5.1.1
  class classname1
    relay target 10.1.1.1
  class classname2
    relay target 10.2.2.2
  class classname3
```

In the above example, classname1 relays the DHCP DISCOVER packet to the server at 10.1.1.1, while classname2 relays the DHCP DISCOVER packet to the server at 10.2.2.2.

If the SG returned classname3, then the default pool at 10.5.1.1 is used. If the SG returns any other class name other than classname1, classname2, or classname3, then no relay action is taken.

The relay target configuration with respect to any configured DHCP pool works in the exact same way as a relay destination configuration works.

Related Commands

Command	Description
relay destination	Configures an IP address for a relay destination to which packets are forwarded by a DHCP server.
relay source	Configures an IP address for a relay source from which packets are forward by a DHCP server.

release dhcp

To perform an immediate release of a Dynamic Host Configuration Protocol (DHCP) lease for an interface, use the **release dhcp** command in user EXEC or privileged EXEC mode.

release dhcp *interface-type interface-number*

Syntax Description

<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>interface-number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(4)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 integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **release dhcp** command immediately releases the DHCP lease on the interface specified by the *interface-type* and *interface-number* arguments. If the router interface was not assigned a DHCP IP address by the DHCP server, the **release dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

This command does not have a **no** form.

Examples

The following example shows how to release a DHCP lease for an interface.

```
release dhcp ethernet 3/1
```

Related Commands

Command	Description
ip address dhcp	Specifies that the Ethernet interface acquires an IP address through DHCP.
lease	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
renew dhcp	Forces the renewal of the DHCP lease for the specified interface.
show dhcp lease	Displays the DHCP addresses leased from a server.
show interface	Displays statistics for all interfaces configured on the router or access server.

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip interface	Displays a summary of an interface's IP information and status.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.
show startup-config	Displays the contents of the configuration file that will be used at the next system startup.

renew deny unknown

To configure the renewal policy for unknown DHCP clients, use the **renew deny unknown** command in DHCP pool configuration mode. To disable the renewal policy, use the no form of this command.

renew deny unknown

no renew deny unknown

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP server ignores a client request for an IP address that is not leased to the client.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.2 SXH	This command was integrated into 12.2 SXH.

Usage Guidelines

In some usage scenarios, such as a wireless hotspot, where both DHCP and secure ARP are configured, a connected client device might go to sleep or suspend for a period of time. If the suspended time period is greater than the secure ARP timeout (default of 91 seconds), but less than the DHCP lease time, the client can awake with a valid lease, but the secure ARP timeout has caused the lease binding to be removed because the client has been inactive. When the client awakes, the client still has a lease on the client side but is blocked from sending traffic. The client will try to renew its IP address but the DHCP server will ignore the request because the DHCP server has no lease for the client. The client must wait for the lease to expire before being able to recover and send traffic again.

To remedy this situation, use the **renew deny unknown** command in DHCP pool configuration mode. This command forces the DHCP server to reject renewal requests from clients if the requested address is present at the server but is not leased. The DHCP server sends a DHCPNAK denial message to the client, which forces the client back to its initial state. The client can then negotiate for a new lease immediately, instead of waiting for its old lease to expire.

Examples

The following example shows how to secure ARP table entries to DHCP leases. The **renew deny unknown** command allows the DHCP server to renew the lease of a DHCP client whose lease has been cleared because of a secure ARP timeout.

```
Router# configure terminal
Router(config)# ip dhcp pool red
Router(dhcp-config)# update arp
Router(dhcp-config)# renew deny unknown
```

renew deny unknown**Related Commands**

Command	Description
update arp	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

renew dhcp

To perform an immediate renewal of a Dynamic Host Configuration Protocol (DHCP) lease for an interface, use the **renew dhcp** command in user EXEC or privileged EXEC mode.

renew dhcp *interface-type interface-number*

Syntax Description		
<i>interface-type</i>		Interface type. For more information, use the question mark (?) online help function.
<i>interface-number</i>		Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	12.3(4)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 integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines The **renew dhcp** command immediately renews the DHCP lease for the interface specified by the *interface-type* and *interface-number* arguments. If the router interface was not assigned an IP address by the DHCP server, the **renew dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

This command does not have a **no** form.

Examples The following example shows how to renew a DHCP lease for an interface:

```
renew dhcp Ethernet 3/1
```

Related Commands	Command	Description
	ip address dhcp	Specifies that the Ethernet interface acquires an IP address through DHCP.
	lease	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
	release dhcp	Releases the DHCP lease on the specified interface.
	show dhcp lease	Displays the DHCP addresses leased from a server.
	show interface	Displays statistics for all interfaces configured on the router or access server.

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip interface	Displays a summary of an interface's IP information and status.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface.
show startup-config	Displays the contents of the configuration file that will be used at the next system startup.

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)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.

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.

service dhcp

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

service dhcp

no service dhcp

Syntax Description This command has no arguments or keywords.

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

Command Modes Global configuration (config)

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

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

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

Examples

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

```
service dhcp
```

Related Commands

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

set ip next-hop dynamic dhcp

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

set ip next-hop dynamic dhcp

no set ip next-hop dynamic dhcp

Syntax Description This command has no arguments or keywords.

Defaults This command is disabled by default.

Command Modes Route-map configuration

Command History

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

Usage Guidelines

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

Examples

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

```
access list 101 permit icmp any host 172.16.23.7 echo
route map MY-LOCAL-POLICY permit 10
match ip address 101
set ip next-hop dynamic dhcp
!
ip local policy route-map MY-LOCAL-POLICY
```

Related Commands

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

show 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 <i>ip-address</i> 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 <i>vrf-name</i> 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	IP Address Assignment Example
	The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, the type of address assignment that has occurred, and the option 82 suboptions of the remote ID and circuit ID.

Table 17 describes the significant fields shown in the displays.

```
Router# show ip dhcp binding 192.0.2.2
```

```
IP address          Client-ID/
                   Hardware address/
                   User name
192.0.2.2           aabb.cc00.0a00      Apr 28 2010 05:00 AM  Automatic
Remote id : 020a00001400006400000000
```

Table 17 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.

Subnet Allocation Example

The following example shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default):

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

```
Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   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
```

Table 18 describes the significant fields shown in the display.

Table 18 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** command in user 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.
<i>vrf-name</i>	(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 <i>vrf-name</i> 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
```

[Table 19](#) describes the fields shown in the display.

Table 19 *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 [Table 19](#) 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

<i>url</i>	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename • flash://filename • disk0://filename
------------	--

Defaults

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

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
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. [Table 20](#) 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 20 *show ip dhcp database Field Descriptions*

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

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

```
show ip dhcp limit lease [type number]
```

Syntax Description

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

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

```
Router# show ip dhcp limit lease

DHCP limit lease logging is enabled
Interface      Count
Serial0/0.1    5
Serial1        3
```

Related Commands

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

show ip dhcp pool

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

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

Syntax Description

name (Optional) Name of the address pool.

Command Default

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

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

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

Examples

The following example shows DHCP address pool information for an on-demand address pool (ODAP), pool 1. [Table 21](#) 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. [Table 21](#) 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 21 *show ip dhcp pool Field Descriptions*

Field	Description
Pool	The name of the pool.
Utilization mark (high/low)	The configured high and low utilization level for the pool.
Subnet size (first/next)	The size of the requested subnets.
VRF name	The VRF name to which the pool is associated.
Total addresses	The total number of addresses in the pool.
Leased addresses	The number of leased addresses in the pool.
Pending event	Displays any pending events.
2 subnets are currently in the pool	The number of subnets allocated to the address pool.
Current index	Displays the current index.
IP address range	The IP address range of the subnets.
Leased addresses	The number of leased addresses from each subnet.
Excluded addresses	The number of excluded addresses.
Interface Ethernet0/0 address assignment	The first line is the primary IP address of the interface. The second line is the secondary IP address of the interface. More than one secondary address on the interface is supported.

Related Commands

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

show ip dhcp relay information trusted-sources

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

show ip dhcp relay information trusted-sources

Syntax Description This command has no arguments or keywords.

Command Modes
user EXEC
privileged EXEC

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

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

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

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

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

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

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

```
All interfaces are trusted source of relay agent information option Serial4/1.1
```

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

show ip dhcp server statistics

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

show ip dhcp server statistics

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

show ip dhcp server statistics [*type number*]

Syntax Description

<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(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 <i>type</i> and <i>number</i> arguments were added. The command was enhanced to display interface level DHCP statistics.

Examples

The following example displays DHCP server statistics. [Table 22](#) 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
DHCPCDISCOVER         200
DHCPCREQUEST          178
DHCPCDECLINE          0
```

show ip dhcp server statistics

```

DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            12
DHCPOFFER            190
DHCPACK              172
DHCNPAK              6

```

Table 22 *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.
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.

Defaults 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.
	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.

Command	Description
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		
<i>ip-address</i>	(Optional) IP address for the binding entries.	
<i>mac-address</i>	(Optional) MAC address for the binding entries.	
vlan <i>vlan</i>	(Optional) Specifies a valid VLAN number; valid values are from 1 to 4094.	
interface <i>type</i>	(Optional) Specifies the interface type; possible valid values are ethernet , fastethernet , gigabitethernet , and tengigabitethernet .	
<i>number</i>	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
```

show ip dhcp snooping binding

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

[Table 23](#) describes the fields in the `show ip dhcp snooping` command output.

Table 23 *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
<code>ip dhcp snooping</code>	Globally enables DHCP snooping.
<code>ip dhcp snooping binding</code>	Sets up and generates a DHCP binding configuration to restore bindings across reboots.
<code>ip dhcp snooping database</code>	Configures the DHCP-snooping database.
<code>ip dhcp snooping information option</code>	Enables DHCP option 82 data insertion.
<code>ip dhcp snooping limit rate</code>	Configures the number of the DHCP messages that an interface can receive per second.

Command	Description
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.

Defaults 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 Succeeded 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 Succeeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts      :      21   Startup Failures :      0
Successful Transfers :      0   Failed Transfers :     21
Successful Reads    :      0   Failed Reads    :      0
Successful Writes   :      0   Failed Writes   :     21
Media Failures     :      0

First successful access: Read

Last ignored bindings counters :
Binding Collisions   :      0   Expired leases   :      0
Invalid interfaces  :      0   Unsupported vlans :      0
Parse failures      :      0

Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions   :      0   Expired leases   :      0
Invalid interfaces  :      0   Unsupported vlans :      0
Parse failures      :      0

```

Related Commands

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

show ip dhcp vrf

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

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

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

Command Modes	
	User EXEC (>) Privileged EXEC (#)

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

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

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

```
Router# show ip dhcp vrf red binding *

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

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

```
Router# show ip dhcp vrf red binding 192.0.2.2

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

Table 24 describes the significant fields shown in the displays.

Table 24 *show ip dhcp vrf Field Descriptions*

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

Related Commands

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

show ip 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.
<i>vrf-name</i>	(Optional) Name of the VRF.
<i>ip-address</i>	(Optional) Address about which routing information should be displayed.

Defaults

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.

snmp-server enable traps dhcp

To enable DHCP Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps dhcp** command in global configuration mode. To disable DHCP trap notifications, use the **no** form of this command.

```
snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]
```

```
no snmp-server enable traps dhcp [duplicate] [interface] [pool] [subnet] [time]
```

Syntax Description

duplicate	(Optional) Sends notification about duplicate IP addresses.
interface	(Optional) Sends notification that a per interface lease limit is exceeded.
pool	(Optional) Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold.
subnet	(Optional) Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold.
time	(Optional) Sends notification that the DHCP server has started or stopped.

Command Default

DHCP trap notifications are not sent.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If you do not specify any of the optional keywords, all DHCP trap notifications are enabled.

Examples

The following example shows how to send SNMP trap notifications to the SNMP manager when the secondary subnet utilization falls below or exceeds the configured threshold:

```
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
!
Router(config)# snmp-server enable traps dhcp subnet
```

In the following example, all DHCP trap notifications will be sent to the SNMP manager in response to DHCP server events:

```
!  
Router(config)# snmp-server enable traps dhcp
```

subnet prefix-length

To configure a subnet allocation pool and determine the size of subnets that are allocated from the pool, use the **subnet prefix-length** command in DHCP pool configuration mode. To unconfigure subnet pool allocation, use the **no** form of this command.

subnet prefix-length *prefix-length*

no subnet prefix-length *prefix-length*

Syntax Description

<i>prefix-length</i>	Configures the IP subnet prefix length in classless interdomain routing (CIDR) bit count notation. The range is from 1 to 31.
----------------------	---

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)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 integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

This command is used to configure a Cisco IOS router as a subnet allocation server for a centralized or remote Virtual Private Network (VPN) on-demand address pool (ODAP) manager. This command is configured under a DHCP pool. The *prefix-length* argument is used to determine the size of the subnets that are allocated from the subnet allocation pool. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation format.

Configuring Global Subnet Pools

Global subnet pools are created in a centralized network. The ODAP server allocates subnets from the subnet allocation server based on subnet availability. When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP server requires the address space. The binding is destroyed and the subnet is returned to the subnet pool only when the ODAP server releases the subnet as address space utilization decreases.

Configuring VPN Subnet Pools

A subnet allocation server can be configured to assign subnets from VPN subnet allocation pools for Multiprotocol Label Switching (MPLS) VPN clients. VPN routes between the ODAP manager and the subnet allocation server are configured based on VRF name or VPN ID configuration. The VRF and VPN ID are configured to maintain routing information that defines customer VPN sites. This customer site is attached to a provider edge (PE) router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

Configuring VPN Subnet Pools for VPN clients with VPN IDs

A subnet allocation server can also be configured to assign subnets from VPN subnet allocation pools based on the VPN ID of a client. The VPN ID (or Organizational Unique Identifier [OUI]) is a unique identifier assigned by the IEEE. VPN routes between the ODAP manager and the subnet allocation server are enabled by configuring the DHCP pool with a VPN ID that matches the VPN ID that is configured for the VPN client.

Examples

Global Configuration Example

The following example configures a router to be a subnet allocation server and creates a global subnet allocation pool named GLOBAL-POOL from the 10.0.0.0 network. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 254 host IP addresses.

```
ip dhcp pool GLOBAL-POOL
 network 10.0.0.0 255.255.255.0
 subnet prefix-length 24
```

VPN Configuration Example

The following example configures a router to be a subnet allocation server and creates a VPN routing and forwarding (VRF) subnet allocation pool named VRF-POOL from the 172.16.0.0 network and configures the VPN to match the VRF named pool1. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 62 host IP addresses.

```
ip dhcp pool VRF-POOL
 vrf pool1
 network 172.16.0.0 /16
 subnet prefix-length 26
```

VPN ID Configuration Example

The following example configures a router to be a subnet allocation server and creates a VRF subnet allocation pool named VPN-POOL from the 192.168.0.0 network and configures the VRF named abc. The VPN ID must match the unique identifier that is assigned to the client site. The route target and route distinguisher are configured in the as-number:network number format. The route target and route distinguisher must match. The configuration of the **subnet prefix-length** command in this example configures each subnet that is allocated from the subnet pool to support 30 host IP addresses.

```
ip vrf abc
 rd 100:1
 route-target both 100:1
 vpn id 1234:123456
 !
ip dhcp pool VPN-POOL
 vrf abc
 network 192.168.0.0 /24
 subnet prefix-length /27
```

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.
ip dhcp pool	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
show ip dhcp pool	Displays information about the DHCP pools.

update arp

To secure dynamic Address Resolution Protocol (ARP) entries in the ARP table to their corresponding DHCP bindings, use the **update arp** command in DHCP pool configuration mode. To disable this command and change secure ARP entries to dynamic ARP entries, use the **no** form of this command.

update arp

no update arp

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **update arp** DHCP pool configuration command is used to secure ARP table entries and their corresponding DHCP leases. However, existing active leases are not secured. These leases will remain insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If this feature is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

This command can be configured only under the following conditions:

- DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.
- Directly connected clients on LAN interfaces and wireless LAN interfaces.

The configuration of this command is not visible to the client. When this command is configured, secured ARP table entries that are created by a DHCP server cannot be removed from the ARP table by the **clear arp-cache** command. This is designed behavior. If a secure ARP entry created by the DHCP server must be removed, the **clear ip dhcp binding** command can be used. This command will clear the DHCP binding and secured ARP table entry.



Note

This command does not secure ARP table entries for BOOTP clients.

Examples

The following example configures the Cisco IOS DHCP server to secure ARP table entries to their corresponding DHCP leases within the DHCP pool named WIRELESS-POOL:

```
ip dhcp pool WIRELESS-POOL
  update arp
```

Related Commands

Command	Description
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP Server database.

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

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

Defaults

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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

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.

Defaults

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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

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.

vrf (DHCP pool)

To associate the on-demand address pool with a VPN routing and forwarding instance (VRF) name, use the **vrf** command in DHCP pool configuration mode. To remove the VRF name, use the **no** form of this command.

vrf *name*

no vrf *name*

Syntax Description

<i>name</i>	Name of the VRF to which the address pool is associated.
-------------	--

Defaults

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Associating a pool with a VRF allows overlapping addresses with other pools that are not on the same VRF. Only one pool can be associated with each VRF. If the pool is configured with the **origin dhcp** command or **origin aaa** command, the VRF information is sent in the subnet request. If the VRF is configured with an RFC 2685 VPN ID, the VPN ID will be sent instead of the VRF name.

Examples

The following example associates the on-demand address pool with a VRF named pool1:

```
ip dhcp pool pool1
  origin dhcp subnet size initial 24 autogrow 24
  utilization mark high 85
  utilization mark low 15
  vrf pool1
```

Related Commands

Command	Description
origin	Configures an address pool as an on-demand address pool.