lease through renew dhcp

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to a DHCP client, use the **lease** command in DHCP pool configuration mode. To restore the default value, use the no form of this command.

lease {*days* [*hours* [*minutes*]]| **infinite**}

no lease

Syntax Description

days	Specifies the duration of the lease in numbers of days.
hours	(Optional) Specifies the number of hours in the lease. A *days* value must be supplied before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. A *days* value and an *hours* value must be supplied before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Command Default

1 day

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.

Examples

The following example shows a 1-day lease:

```
lease 1
```

The following example shows a 1-hour lease:

```
lease 0 1
```

The following example shows a 1-minute lease:

```
lease 0 0 1
```

The following example shows an infinite (unlimited) lease:

```
lease infinite
```

Related Commands

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

local-ip (IPC transport-SCTP local)

To define at least one local IP address that is used to communicate with the local peer, use the **local-ip**command in IPC transport-SCTP local configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

local-ip *device-real-ip-address* [*device-real-ip-address2*]

no local-ip *device-real-ip-address* [*device-real-ip-address2*]

Syntax Description

device-real-ip-address	IP address of the local device. The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
device-real-ip-address2	(Optional) IP address of the local device.

Command Default

No IP addresses are defined; thus, peers cannot communicate with the local peer.

Command Modes

IPC transport-SCTP local configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **local-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switchover (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
```

```
no shutdown
protocol sctp
 local-port 5000
  local-ip 10.0.0.1
 remote-port 5000
  remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port number that is used to communicate with the redundant peer.
remote-ip	Defines at least one remote IP address that is used to communicate with the redundant peer.

local-port

To define the local Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **local-port**command in SCTP protocol configuration mode.

local-port *local-port-number*

Syntax Description

local-port-number	Local port number, which should be the same as the remote port number on the peer router (which is specified via the **remote-port** command).

Command Default

A local SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **local-port** command enters IPC transport-SCTP local configuration mode, which allows you to specify at least one local IP address (via the **local-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
!
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.

Command	Description
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

logging (cfg-dns-view)

To enable logging of a system message logging (syslog) message each time the Domain Name System (DNS) view is used, use the **logging** command in DNS view configuration mode. To disable logging of a syslog message each time the DNS view is used, use the **no** form of this command.

logging

no logging

Syntax Description

This command has no arguments or keywords.

Command Default

No syslog message is logged when the DNS view is used.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables the logging of syslog messages for the DNS view.

To display the logging setting for a DNS view, use the **show ip dns view** command.

Examples

The following example shows how to enable logging of a syslog message each time the DNS view named user3 that is associated with the VRF vpn32 is used:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# logging
```

Related Commands

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

logging (DNS)

To enable logging of a system message logging (syslog) message each time the Domain Name System (DNS) view is used, use the **logging** command in DNS view configuration mode. To disable logging of a syslog message each time the DNS view is used, use the **no** form of this command.

logging

no logging

Syntax Description

This command has no arguments or keywords.

Command Default

No syslog message is logged when the DNS view is used.

Command Modes

DNS view configuration

Command History

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

Usage Guidelines

This command enables the logging of syslog messages for the DNS view.

To display the logging setting for a DNS view, use the **show ip dns view** command.

Examples

The following example shows how to enable logging of a syslog message each time the DNS view named user3 that is associated with the VRF vpn32 is used:

```
Router(config)# ip dns view vrf vpn32 user3
Router(cfg-dns-view)# logging
```

Related Commands

Command	Description
ip dns view	Enters DNS view configuration mode for the specified DNS view so that the logging setting, forwarding parameters, and resolving parameters can be configured for the view.
show ip dns view	Displays information about a particular DNS view or about all configured DNS views, including the number of times the DNS view was used.

logging server-arp

To enable the sending of Address Resolution Protocol (ARP) requests for syslog server address during system initialization bootup, use the **logging server-arp** command in global configuration mode. To disable the sending of ARP requests for syslog server addresses, use the **no** form of this command.

logging server-arp

no logging server-arp

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.3	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(5)B	This command was integrated into Cisco IOS Release 12.3(5)B.

Usage Guidelines

The **logging server-arp** global configuration command allows the sending of ARP requests for syslog server addresses during system initialization bootup.

When this CLI command is configured and saved to the startup configuration file, the system will send an ARP request for remote syslog server address before sending out the first syslog message.

The command should only be used when the remote syslog server is in the same subnet as the system router sending the ARP request.

Note Use this command even if a static ARP has been configured with the remote syslog server address.

Examples

The following example shows how to enable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# logging server-arp
Router(config)# exit
```

The following example shows how to disable an ARP request for syslog server addresses:

```
Router# configure terminal
Router(config)# no
 logging server-arp
Router(config)# exit
```

Related Commands

Command	Description
arp (global)	Adds a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode.

mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **mac packet-classify** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify [bpdu]

no mac packet-classify [bpdu]

Syntax Description

bpdu	(Optional) Specifies Layer 2 policy enforcement for BPDU packets.

Command Default

Layer 3 packets are not classified as Layer 2 packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)SXD	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.
12.2(50)SY	Added support for MAC ACLs on BPDU packets.

Usage Guidelines

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

You can configure these interface types for multilayer MAC access control list (ACL) quality of service (QoS) filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support Ethernet over Multiprotocol Label Switching (EoMPLS)
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **mac packet-classify** command enabled.

The **mac packet-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q class of service (CoS), trunk VLAN, EtherType, and MAC addresses.

Examples

This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

This example shows how to enforce Layer 2 policies on BPDU packets:

```
Router(config-if)# mac packet-classify bpdu
Router(config-if)#
```

This example shows how to disable Layer 2 policies on BPDU packets:

```
Router(config-if)# no mac packet-classify bpdu
Router(config-if)#
```

Related Commands

Command	Description
mac packet-classify use vlan	Enables VLAN-based QoS filtering in the MAC ACLs.

mac packet-classify use vlan

To enable VLAN-based quality of service (QoS) filtering in the MAC access control lists (ACLs), use the **mac packet-classify use vlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mac packet-classify use vlan

no mac packet-classify use vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-based QoS filtering in the MAC ACLs is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

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

You must use the **no mac packet-classify use vlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 Service Advertising Protocol (SAP)-encoded packets (for example, Intermediate System-to-Intermediate System [IS-IS] and Internet Packet Exchange [IPX]).

QoS does not allow policing of non-Advanced Research Protocol Agency (ARPA) Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

Examples

This example shows how to enable Layer 2 classification of IP packets:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable Layer 2 classification of IP packets:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

Related Commands

Command	Description
mac packet-classify	Classifies Layer 3 packets as Layer 2 packets.

match message-type

To configure parameters for a service-list based on a message type, use the **match message-type** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a message type, use the **no** form of this command.

match message-type {**announcement** | **any** | **query**}

no match message-type

Syntax Description

announcement	Filters a service-list according to periodic mDNS announcements sent out by a device.
any	Filters a service-list for queries and announcements.
query	Filters a service-list according to associated queries.

Command Default

A service-list is not filtered for a query or announcement.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **match message-type** command must be used after a service-list is created, and the permit or deny option is exercised.

Examples

The following example shows how to filter a service-list for the announcement message type.:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match message-type announcement
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match service-instance	Configures parameters for a service-list, for a specified service-instance.
match service-type	Configures parameters for a service-list, for a specified service-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

match reply prefix-list

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

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

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

Syntax Description

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

Command Default

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

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

match server access-list

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

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

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

Syntax Description

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

Command Default

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

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

match service-instance

To configure parameters for a service-list based on a service-instance, use the **match service-instance** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a service-instance, use the **no** form of this command.

match service-instance *instance-name*

no match service-instance

Syntax Description

instance-name	Service instance name. The service-list is filtered according to the specified service-list.

Command Default

A service-list is not filtered for a service-instance name.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **match service-instance** command must be used after a service-list is created, and the permit or deny option is exercised.

Examples

The following example shows how to filter a service-list by a service instance:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match service-instance service1
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match message-type	Configures parameters for a service-list, for a message-type.

Command	Description
match service-type	Configures parameters for a service-list, for a specified service-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

match service-type

To configure parameters for a service-list based on a service-type, use the **match service-type** command in multicast Domain Name System (mDNS) service discovery service-list mode. To disable configuration of parameters for a service-list based on a service-type, use the **no** form of this command.

match service-type *mDNS-service-type-string*

no match service-type

Syntax Description

mDNS-service-type-string	Service type string. The service-list is filtered for the specified service-type.

Command Default

A service-list is not filtered for a service-type.

Command Modes

mdns service discovery service-list (config-mdns-sd-sl)

Command History

Release	Modification
15.2(1)E	This command was introduced.

Usage Guidelines

The **match service-type** command must be used after a service-list is created, and the permit or deny option is exercised.

Examples

The following example shows how to filter a service-list for a TXT service-type:

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match service-type TXT
Device(config-mdns-sd-sl)# exit
```

Related Commands

Command	Description
service-list mdns-sd	Creates a service-list and applies a filter on the service-list or associates a query for the service-list.
match service-instance	Configures parameters for a service-list, for a service-instance.

Command	Description
match message-type	Configures parameters for a service-list, for a message-type.
show mdns statistics	Displays mDNS statistics for the specified service-list.

mode (nat64)

To configure the Network Address Translation 64 (NAT64) mapping of addresses and ports (MAP-T) mode, use the **mode** command in NAT64 MAP-T configuration mode. To exit from the NAT64 MAP-T mode, use the **no** form of this command.

mode {**divi** | **map-t**}

no mode

Syntax Description

divi	Configures the stateless dual translation mode.
map-t	Configures the MAP-T mode. This mode is the default.

Command Default

MAP-T is the default mode.

Command Modes

NAT64 MAP-T configuration (config-nat64-mapt)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

In dual translation mode, IPv4 is translated into IPv6 and vice versa.

Examples

The following example shows how to configure the dual translation mode for stateless NAT64:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# mode divi
```

Related Commands

Command	Description
nat64 map-t	Configures NAT64 MAP-T settings.

name

To configure the redundancy group with a name, use the **name**command in redundancy application group configuration mode. To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*

no name *group-name*

Syntax Description

group-name	Name of the redundancy group.

Command Default

The redundancy group is not configured with a name.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

nat64 enable

To enable Network Address Translation 64 (NAT64) on an interface, use the **nat64 enable** command in interface configuration mode. To disable the NAT64 configuration on an interface, use the **no** form of this command.

nat64 enable

no nat64 enable

Syntax Description

This command has no arguments or keywords.

Command Default

NAT64 is not enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Examples

The following example shows how to enable NAT64 on a Gigabit Ethernet interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet0/0/0
Device(config-if)# nat64 enable
Device(config-if)# end
```

Related Commands

Command	Description
show nat64 adjacency	Displays information about the NAT64-managed adjacencies.
show nat64 ha status	Displays information about the NAT64 HA status.
show nat64 statistics	Displays statistics about a NAT64 interface and the transmitted and dropped packet count.

nat64 logging

To enable Network Address Translation 64 (NAT64) high-speed logging (HSL), use the **nat64 logging** command in global configuration mode. To disable NAT64 logging, use the **no** form of this command.

nat64 logging translations flow-export v9 udp destination *hostname port*

no nat64 logging translations

Syntax Description

translations	Enables NAT64 translation logging.
flow-export	Enables NAT64 logging through flow export.
v9	Enables Version 9 NetFlow export format logging.
udp	Enables logging of UDP packets.
destination	Specifies the NAT64 external logging destination.
hostname	Hostname or the IPv4 address of the external collector for logging records.
port	Port number of the IPv4 host of the external collector for logging records. Valid values are from 1 to 65535.

Command Default

NAT64 logging is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The **nat64 logging** command allows you to specify remote logging for NAT64 objects.

The **nat64 logging** command is based on the NetFlow Version 9 export format.

In Cisco IOS XE Release 3.4S and later releases, NAT supports HSL. When HSL is configured, NAT provides a log of the packets that are flowing through the routing devices (similar to the Version 9 NetFlow-like records) to an external collector.

Examples

The following example shows how to enable NAT64 HSL logging:

```
Router(config)# nat64 logging translations flow-export v9 udp destination 10.1.1.1 2000
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 logging translations

Syntax Description

Command Default

Command Modes

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

nat64 map-t

To configure the Network Address Translation 64 (NAT64) mapping of addresses and ports translation (MAP-T) settings, use the **nat64 map-t** command in global configuration mode. To remove the NAT64 MAP-T settings, use the **no** form of this command.

nat64 map-t domain *number*

no nat64 map-t domain *number*

Syntax Description

domain *number*	Specifies the NAT64 MAP-T domain. Valid values for the *number* argument are from 1 to 128.

Command Default

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

After you configure the **nat64 map-t** command, the command mode changes to NAT64 MAP-T configuration mode.

Examples

The following example shows how to configure NAT64 MAP-T settings:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-map-t)#
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
default-mapping-rule	Configures NAT64 MAP-T domain default mapping rule.

nat64 prefix stateful

To configure a prefix and a prefix length for stateful Network Address Translation 64 (NAT64), use the **nat64 prefix stateful** command in global configuration or interface configuration mode. To disable the configuration, use the **no** form of this command.

nat64 prefix stateful *ipv6-prefix*/*prefix-length*

no nat64 prefix stateful *ipv6-prefix*/*prefix-length*

Syntax Description

ipv6-prefix	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/*prefix-length*	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

NAT64 stateful prefixes are not configured.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release3.4 S	This command was introduced.

Usage Guidelines

Use the **nat64 prefix stateful** command in global configuration mode to assign a global NAT64 stateful prefix, or use it in interface configuration mode to assign a unique NAT64 stateful prefix for an interface. A maximum of one global stateful prefix and one stateful prefix per interface is supported. If a global stateful prefix or an interface stateful prefix is not configured, the Well Known Prefix (WKP) of 64:ff9b::/96 is used to translate the IPv4 address of the IPv4 host.

Examples

The following example shows how to configure a global NAT64 stateful prefix:

```
Router(config)# nat64 prefix stateful 2001:DB8:0:1::/96
```

The following example shows how to configure a NAT64 stateful prefix for a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# nat64 prefix stateful 2001:DB8:0:1::/96
```

Related Commands

Command	Description
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
show nat64 prefix stateful	Displays information about NAT64 stateful prefixes.

nat64 prefix stateless

To assign a global or interface-specific Network Address Translation 64 (NAT64) stateless prefix, use the **nat64 prefix stateless** command in global configuration or interface configuration mode. To disable the configuration, use the **no** form of this command.

nat64 prefix stateless *ipv6-prefix*/*prefix-length*

no nat64 prefix stateless

Syntax Description

ipv6-prefix	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No NAT64 translation is performed.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

The **nat64 prefix stateless** command uses a prefix and prefix length for IPv4-translatable IPv6 addresses. Use the **nat64 prefix stateless** command in global configuration mode to assign a global NAT64 stateless prefix or in interface configuration mode to assign an unique NAT64 stateless prefix for each interface. In interface configuration mode, a stateless prefix should be configured on an IPv6-facing interface.

All packets coming to an IPv6 interface are matched against the configured prefix, and the matched packets are translated to IPv4. Similarly, the packets that the IPv6 interface sends use the stateless prefix to construct the source and destination IPv6 address.

Note A maximum of one global stateless prefix and one stateless prefix per interface is supported.

If NAT64 is enabled on an interface that does not have a stateless prefix configured, then the global stateless prefix is used. However, if a global prefix and an interface prefix are configured, then the interface prefix is used for stateless NAT64 translation. The use of a stateless prefix on an interface has priority over the configured global stateless prefix.

Examples

The following example shows how to configure a global NAT64 stateless prefix:

```
Device# configure terminal
Device(config)# nat64 prefix stateless 2001::DB8::1/96
Device(config)# end
```

The following example shows how to assign a NAT64 stateless prefix for a Gigabit Ethernet interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet0/0/0
Device(config-if)# nat64 prefix stateless 2001:0DB8:0:1::/96
Device(config-if# end
```

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.
show nat64 prefix stateless	Displays information about the configured NAT64 stateless prefixes.

nat64 route

To specify the Network Address Translation 64 (NAT64) prefix to which an IPv4 prefix should be translated, use the **nat64 route** command in global configuration mode. To disable the configuration, use the **no** form of this command.

nat64 route *ipv4-prefix*/*mask interface-type interface-number*

no nat64 route *ipv4-prefix*/*mask*

Syntax Description

ipv4-prefix / *mask*	Length of the IPv4 prefix and the mask.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	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 NAT64 routing is performed.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

A prefix that is configured on an interface is used as the stateless prefix on that interface. If no interface-specific prefix is configured, the configured global prefix is used for NAT64 translation.

Examples

The following example shows how to assign an IPv4 prefix and mask to an interface:

```
Device# configure terminal
Device(config)# nat64 route 192.168.0.0/24 gigabitethernet0/0/1
Device(config)# exit
```

Related Commands

Command	Description
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
show nat64 routes	Displays information about the configured NAT64 routes.

nat64 service ftp

To enable the Network Address Translation 64 (NAT64) FTP service, use the **nat64 service ftp** command in global configuration mode. To disable the NAT64 FTP service, use the **no** form of this command.

nat64 service ftp

no nat64 service ftp

Syntax Description

This command has no arguments or keywords.

Command Default

The NAT64 FTP service is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Service FTP is an application-level gateway (ALG) that helps NAT64 operate on Layer 7 data.

Examples

The following example shows how to disable the NAT64 FTP service:

```
Router(config)# no nat64 service ftp
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 settings

To configure Network Address Translation 64 (NAT64) settings, use the **nat64 settings** command in global configuration mode. To disable NAT64 settings, use the **no** form of this command.

nat64 settings {**fragmentation header disable**| **v4 tos ignore**}

no nat64 settings {**fragmentation header disable**| **v4 tos ignore**}

Syntax Description

fragmentation header disable	Disables the NAT64 fragmentation header.
v4 tos ignore	Specifies not to copy the IPv4 type-of-service (ToS) header.

Command Default

NAT64 settings are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

By default, NAT64 adds a fragmentation header for all IPv4-to-IPv6 packets that do not have the Do Not Fragment (DF) bits set. Configure the **nat64 settings fragmentation header disable** command to disable the adding of a fragmentation header for packets that are not fragmented.

By default, NAT64 copies ToS bits from an IPv4 header to an IPv6 header. Configure the **nat64 settings v4 tos ignore** command to disable the copying of ToS bits from an IPv4 header to IPv6 header.

Examples

The following example shows how to disable the NAT64 fragmentation header:

```
Router(config)# nat64 settings fragmentation header disable
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 settings eif

To enable the Network Address Translation 64 (NAT64) end-point independent filtering (EIF), use the **nat64 settings eif** command in global configuration mode. To disable the EIF settings, use the **no** form of this command.

nat64 settings eif enable

no nat64 settings eif enable

Syntax Description

enable	Enables EIF settings.

Command Default

NAT64 EIF settings are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Examples

The following example shows how to enable the NAT64 EIF:

```
Device(config)# nat64 settings eif enable
```

Related Commands

Command	Description
nat64 settings	Configures NAT64 settings

nat64 settings flow-entries disable

To disable flow cache entries in Network Address Translation 64 (NAT64) configurations, use the **nat64 settings flow-entries disable** command in global configuration mode. To enable flow cache entries in NAT64 configurations, use the **no** form of this command.

nat64 settings flow-entries disable

no nat64 settings flow-entries disable

Syntax Description

This command has no arguments or keywords.

Command Default

Flow cache entries are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

Note Disabling flow cache entries will result in lesser performance as this functionality performs multiple database searches to find the most specific translation to use.

By default, Network Address Translation (NAT) creates a session (which is a 5-tuple entry) for every translation. A session is also called a flow cache entry.

NAT64 (stateful and stateless) translations support the disabling of flow cache entries. You can disable flow cache entries in dynamic and static NAT64 configurations. Instead of creating sessions, dynamic and static NAT64 translations can translate a packet off the binding (or bindings if both inside and outside bindings are available). A binding or a half entry is an association between a local IP address and a global IP address.

Disabling flow cache entries for dynamic and static translations saves memory usage and provides more scalability for your NAT64 translations.

Note Port Address Translation (PAT) or interface overload does not support disabling of flow cache entries.

Examples

The following example shows how to enable flow cache entries in a static NAT64 configuration:

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# nat64 prefix stateful 2001:DB8:1::1/96
```

```
Device(config)# nat64 v6v4 static 2001:DB8:1::FFFE 209.165.201.1
Device(config)# no nat64 settings flow-entries disable
```

Related Commands

Command	Description
ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
nat64 prefix stateful	Configures a prefix and a prefix length for stateful NAT64.
nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.

nat64 settings mtu minimum

To set the minimum size for the Network Address Translation 64 (NAT64) maximum transmission units (MTU), use the **nat64 settings mtu minimum** command in interface configuration mode. To return to the default MTU size of 1280 bytes, use the **no** form of this command.

nat64 settings mtu minimum *size*

no nat64 settings mtu minimum

Syntax Description

size	Minimum MTU in bytes. The range is from 1281 to the MTU of the interface.

Command Default

The default value is 1280 bytes, which is the minimum MTU on an IPv6 link.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. The MTU size of an interface defaults to the largest size possible for that interface type. To adjust the MTU size of an interface, configure the **mtu** command. Packets are fragmented based on the configured MTU size.

If the Do Not Fragment (DF) bits are not set, during the NAT64 translation and fragmentation of IPv4 packets to IPv6, NAT64 assumes that the IPv6 link minimum MTU size is 1280 bytes. However, the link MTU size could be greater than the minimum IPv6 link MTU size. To better utilize the network, network administrators can use the **nat64 settings mtu minimum** command to set a higher minimum MTU size. For example, if interfaces in a network are all Ethernet interfaces and the MTU size is 1500 bytes, fragmenting packets at 1280 bytes is not an effective utilization of the bandwidth. In this case, the network administrator can change the MTU size to 1500 bytes. When the **nat64 settings mtu minimum** command is configured, NAT64 ignores the implicit minimum MTU of 1280 bytes and fragments IPv6 packets based on the configured MTU size.

Note The **nat64 settings mtu minimum** command works only on IPv6-facing interfaces.

Examples

The following example shows how to configure a minimum MTU size of 1450 bytes for Gigabit Ethernet interface 0/0/1:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# nat64 settings mtu minimum 1450
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
mtu	Adjusts the maximum packet size or MTU size.

nat64 switchover replicate http

To replicate the Network Address Translation 64 (NAT64) HTTP switchover settings, use the **nat64 switchover replicate http** command in global configuration mode. To disable the HTTP switchover replication settings, use the **no** form of this command.

nat64 switchover replicate http {**enable** | **disable**} **port** *port-number*

no nat64 switchover replicate http

Syntax Description

disable	Disables HTTP session replication.
enable	Enables HTTP session replication.
port	Specifies the HTTP port.
port-number	Port number. Valid values are from 1 to 65535.

Command Default

NAT64 HTTP sessions are not replicated.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

In stateful NAT64 intra-chassis redundancy, HTTP sessions are not backed up on the standby Forward Processor (FP). A typical HTTP application has short-lived, transient flows. Because of the transient nature of the HTTP flows, these flows are not replicated. With stateful NAT64 intra-chassis redundancy you have the ability to replicate HTTP sessions so that HTTP flows can be made to live longer. To replicate HTTP sessions on the standby FP during a switchover, you must configure the **nat64 switchover replicate http enable** command.

You can enable and disable the replication of HTTP sessions on ports. For example, you can configure the **nat64 switchover replicate http port 80** command and replicate the switchover of HTTP sessions on port 80. Configure the **nat64 switchover replicate http disable port 8080** command to disable the replication of HTTP sessions on port 8080. You can disable the replication of sessions on only one port at any given time; however, you can enable the replication of sessions on all ports.

Examples

The following example shows how to replicate switchover of NAT64 HTTP sessions:

```
Router(config)# nat64 switchover replicate http enable port 80
```

Related Commands

Command	Description
ip nat switchover replication http	Replicates HTTP sessions during a switchover.

nat64 translation

To enable Network Address Translation 64 (NAT64) translation, use the **nat64 translation** command in global configuration mode. To disable NAT64 translation, use the **no** form of this command.

nat64 translation {**max-entries** *limit*| **timeout** {**icmp**| **tcp**| **tcp-transient**| **udp**} *seconds*}

nat64 translation {**max-entries**| **timeout** {**icmp**| **tcp**| **tcp-transient**| **udp**}}

Syntax Description

max-entries	Configures the maximum number of stateful NAT64 translations allowed on a router.
limit	NAT64 translation entry limit. Valid values are from 1 to 2147483647.
timeout	Specifies the NAT64 translation entry timeout.
icmp	Specifies the timeout for NAT64 Internet Control Message Protocol (ICMP) traffic flow.
tcp	Specifies the timeout for NAT64 established TCP traffic flow.
tcp-transient	Specifies the timeout for NAT64 transient TCP traffic flow.
udp	Specifies the timeout for NAT64 UDP traffic flow.
seconds	Traffic timeout, in seconds. Valid values are from 1 to 536870.

Command Default

NAT64 translation is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The **nat64 translation timeout** command overrides the default aging timeout for NAT64 translations.

A transient TCP session has three possible conditions: a synchronize (SYN) handshake is started, but it is not complete; a reset (RST) packet is received; or a finished (FIN) packet is received in both directions.

Examples

The following example shows how to set the NAT64 translation maximum entry limit to 500:

```
Device(config)# nat64 translation max-entries 500
```

The following example shows how to set the NAT64 translation timeout for TCP to 20,000 seconds:

```
Device(config)# nat64 translation timeout tcp 20000
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 v4

To enable Network Address Translation 64 (NAT64) IPv4 configuration, use the **nat64 v4** command in global configuration mode. To disable the NAT64 IPv4 configuration, use the **no** form of this command.

nat64 v4 pool *pool-name start-address-range end-address-range*

no nat64 v4 pool *pool-name* [**forced**| *start-address-range end-address-range* [**forced**]]

Syntax Description

pool	Configures an IPv4 address pool.
pool-name	Name of the IPv4 address pool.
start-address-range	Starting address of the address pool range.
end-address-range	Ending address of the address pool range.
forced	(Optional) Removes the configuration even when the NAT64 translation exists for the configuration.

Command Default

The NAT64 IPv4 configuration is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

In Cisco IOS XE Release 3.4S, the Stateful NAT64 feature supports only single range pools.

Examples

The following example shows how to enable the NAT64 IPv4 pool configuration:

```
Router(config)# nat64 v4 pool pool1 192.168.0.2 192.168.0.254
```

Related Commands

Command	Description
nat64 enable	Enables NAT64 on an interface.

nat64 v4v6

To translate an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for Network Address Translation 64 (NAT64), use the **nat64 v4v6** command in global configuration mode. To disable the translation, use the **no** form of this command.

nat64 v4v6 static{*ipv4-address ipv6-address*| **tcp** *ipv4-address port ipv6-address port*| **udp** *ipv4-address port ipv6-address port*}[**redundancy** *group-id* **mapping-id** *id*]

no nat64 v4v6 static{*ipv4-address ipv6-address*| [**forced**]| **tcp** *ipv4-address port ipv6-address port*| **udp** *ipv4-address port ipv6-address port*} [**forced**] [**redundancy** *group-id* **mapping-id** *id*]

Syntax Description

static	Associates an IPv6 address to an IPv4 host statically.
ipv4-address	Address of the IPv4 host.
ipv6-address	IPv6 address to which the IPv4 host is mapped to in the IPv6 network.
tcp	Applies static mapping to TCP protocol packets.
port	Port number of the IPv6 or IPv4 address. Valid values are from 1 to 65535.
udp	Applies static mapping to UDP protocol packets.
redundancy *group-id*	(Optional) Configures a redundancy group (RG) with the specified ID. Valid values are 1 and 2.
mapping-id *id*	(Optional) Configures a unique ID for mapping devices. The same ID should be configured on both active and standby devices. Valid values are from 1 to 20480.
forced	(Optional) Removes the configuration even when the NAT64 translation exists for the configuration.

Command Default

NAT64 IPv4-to-IPv6 translation is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. The **redundancy** *group-id* and **mapping-id** *id* keyword-argument pairs were added.

Examples

The following example shows how to enable static mapping of an IPv4 address to an IPv6 address:

```
Device(config)# nat64 v4v6 static 192.168.0.1 2001:DB8:0::1
```

The following example shows how to configure a redundancy group to a static IPv4-to-IPv6 address configuration:

```
Device(config)# nat64 v4v6 static 192.168.0.1 2001:DB8:0::1 redundancy 1 mapping-id 101
```

Related Commands

Command	Description
nat64 v6v4	Translates an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for NAT64.

nat64 v6v4

To translate an IPv6 source address to an IPv4 source address and an IPv4 destination address to an IPv6 destination address for Network Address Translation 64 (NAT64), use the **nat64 v6v4** command in global configuration mode. To disable the translation, use the **no** form of this command.

nat64 v6v4 {**list** *access-list-name* **pool** *pool-name* [**overload**]| **static** {*ipv6-address ipv4-address*| **tcp** *ipv6-address port ipv4-address port*| **udp** *ipv6-address port ipv4-address port*}}[**redundancy** *group-id* **mapping-id** *id*]

no nat64 v6v4 {**list** *access-list-name* **pool** *pool-name* [**overload**]| **static** {*ipv6-address ipv4-address*| **tcp** *ipv6-address port ipv4-address port*| **udp** *ipv6-address port ipv4-address port*}} [**forced**][**redundancy** *group-id* **mapping-id** *id*]

Syntax Description

list	Associates an IPv4 pool with the filtering mechanism that decides when to apply an IPv6 address mapping.
access-list-name	Name of the IPv6 access list.
pool	Specifies the NAT64 pool for dynamic mapping of addresses.
pool-name	Name of the NAT64 pool.
overload	(Optional) Enables NAT64 overload address translation.
static	Enables NAT64 static mapping of addresses.
ipv6-address	IPv6 address of the IPv6 host to which static mapping is applied.
ipv4-address	IPv4 address that represents the IPv6 host for static mapping in the IPv4 network.
tcp	Applies static mapping to TCP protocol packets.
port	Port number of the IPv6 or IPv4 address. Valid values are from 1 to 65535.
udp	Applies static mapping to UDP protocol packets.
redundancy *group-id*	(Optional) Configures a redundancy group (RG). Valid values are 1 and 2.
mapping-id *id*	(Optional) Configures a unique ID for mapping devices. The same ID should be configured on both active and standby devices. Valid values are from 1 to 20480.
forced	(Optional) Removes the configuration even when the NAT64 translation exists for the configuration.

Command Default NAT64 IPv6-to-IPv4 translation is not enabled.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **redundancy** *group-id* and **mapping-id** *id* keyword-argument pairs were added.

Examples The following example shows how to enable dynamic mapping of an IPv6 address to an IPv4 address pool:

```
Device(config)# nat64 v6v4 list list1 pool pool1
```

The following example shows how to configure an RG for a dynamic IPv6-to-IPv4 address pool:

```
Device(config)# nat64 v6v4 list list1 pool pool1 redundancy 1 mapping-id 203
```

Related Commands

Command	Description
nat64 v4v6	Translates an IPv4 source address to an IPv6 source address and an IPv6 destination address to an IPv4 destination address for NAT64.

netbios-name-server

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

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

no netbios-name-server

Syntax Description

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

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

netbios-node-type

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

netbios-node-type *type*

no netbios-node-type

Syntax Description

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

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The recommended type is h-node (hybrid).

Examples

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

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

Related Commands

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

network (DHCP)

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

[1]

[2]

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **secondary** keyword was added.

1

2

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

This command is valid for DHCP subnetwork address pools only.

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

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

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

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

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

Examples

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

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

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

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

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

Router(dhcp-config)#
network 192.0.2.0 255.255.255.0

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

Related Commands

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

next-server

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

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

no next-server *address*

Syntax Description

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

Command Default

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

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Examples

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

```
next-server 10.12.1.99
```

Related Commands

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

nhrp group

To configure a Next Hop Resolution Protocol (NHRP) group on a spoke, use the **nhrp group** command in interface configuration mode. To remove an NHRP group, use the **no** form of this command.

nhrp group *group-name*

no nhrp group *group-name*

Syntax Description

group-name	Specifies an NHRP group name.

Command Default

No NHRP groups are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

After you create an NHRP group on a spoke, you use the **nhrp map group** command to map the group to a QoS policy map.

Note This command will replace the **ip nhrp group** command in a future release.

Examples

The following example shows how to create two NHRP groups named small and large.

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 0
Device(config-if)# nhrp group small
Device(config-if)# nhrp group large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.

Command	Description
nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.
show dmvpn	Displays DMVPN-specific session information.
show nhrp	Displays NHRP mapping information.
show nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

nhrp map group

To associate a Next Hop Resolution Protocol (NHRP) group to a QoS policy map, use the **nhrp map group** command in interface configuration mode. To remove an association, use the **no** form of this command.

nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

no nhrp map group *group-name* **service-policy output** *qos-policy-map-name*

Syntax Description

service-policy	Specifies a QoS service policy
group-name	Specifies an NHRP group name.
qos-policy-map-name	Specifies a QoS policy map name.

Command Default

No mappings are created.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

The command allows a QoS policy in the output direction only.

Note This command will replace the **ip nhrp map group** command in a future release.

Examples

The following example shows how to map two NHRP groups named small and large to two QoS policy maps named qos-small and qos-large respectively.

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 0
Device(config-if)# nhrp map group small service-policy output qos-small
Device(config-if)# nhrp map group large service-policy output qos-large
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
nhrp group	Configures an NHRP group on a spoke.
show dmvpn	Displays DMVPN-specific session information.
show nhrp	Displays NHRP mapping information.
show nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

nis address

To specify the network information service (NIS) address of an IPv6 server to be sent to the client, use the **nis address** command in DHCP for IPv6 pool configuration mode. To remove the NIS address, use the **no** form of this command.

nis address *ipv6-address*

no nis address *ipv6-address*

Syntax Description

ipv6-address	The NIS address of an IPv6 server to be sent to the client.

Command Default

No NIS address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS server option provides a list of one or more IPv6 addresses of NIS servers available to send to the client. The client must view the list of NIS servers as an ordered list, and the server may list the NIS servers in the order of the server's preference.

The NIS server option code is 27. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS address of an IPv6 server:

```
nis address 23::1
```

Related Commands

Command	Description
import nis address	Imports the NIS server option to a DHCP for IPv6 client.
nis domain-name	Enables a server to convey a client's NIS domain name information to the client.

nis domain-name

To enable a server to convey a client's network information service (NIS) domain name information to the client, use the **nis domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nis domain-name *domain-name*

no nis domain-name *domain-name*

Syntax Description

domain-name	The domain name of an IPv6 server to be sent to the client.

Command Default

No NIS domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS domain name option provides a NIS domain name for the client. Use the **nis domain-name** command to specify the client's NIS domain name that the server sends to the client.

The NIS domain name option code is 29. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS domain name of a client:

```
nis domain-name cisco1.com
```

Related Commands

Command	Description
import nis domain	Imports the NIS domain name option to a DHCP for IPv6 client.
nis address	Specifies the NIS address of an IPv6 server to be sent to the client.

nisp domain-name

To enable an IPv6 server to convey a client's network information service plus (NIS+) domain name information to the client, use the **nisp domain-name**command in DHCP for IPv6 pool configuration mode. To remove the domain name, use the **no** form of this command.

nisp domain-name *domain-name*

no nisp domain-name *domain-name*

Syntax Description

domain-name	The NIS+ domain name of an IPv6 server to be sent to the client.

Command Default

No NIS+ domain name is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ domain name option provides a NIS+ domain name for the client. Use the **nisp domain-name** command to enable a server to send the client its NIS+ domain name information.

The NIS+ domain name option code is 30. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to enable the IPv6 server to specify the NIS+ domain name of a client:

```
nisp domain-name cisco1.com
```

Related Commands

Command	Description
import nisp domain	Imports the NIS+ domain name option to a DHCP for IPv6 client.
nisp address	Specifies the NIS+ address of an IPv6 server to be sent to the client.

nisp address

To specify the network information service plus (NIS+) address of an IPv6 server to be sent to the client, use the **nisp address** command in DHCP for IPv6 pool configuration mode. To remove the NIS+ address, use the **no** form of the command.

nisp address *ipv6-address*

no nisp address *ipv6-address*

Syntax Description

ipv6-address	The NIS+ address of an IPv6 server to be sent to the client.

Command Default

No NIS+ address is specified.

Command Modes

IPv6 DHCP pool configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. It was integrated into Cisco IOS XE Release 2.5.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE.

Usage Guidelines

The Dynamic Host Configuration Protocol (DHCP) for IPv6 for stateless configuration allows a DHCP for IPv6 client to export configuration parameters (that is, DHCP for IPv6 options) to a local DHCP for IPv6 server pool. The local DHCP for IPv6 server can then provide the imported configuration parameters to other DHCP for IPv6 clients.

The NIS+ servers option provides a list of one or more IPv6 addresses of NIS+ servers available to send to the client. The client must view the list of NIS+ servers as an ordered list, and the server may list the NIS+ servers in the order of the server's preference.

The NIS+ servers option code is 28. For more information on DHCP options and suboptions, see the "DHCPv6 Options" appendix in the *Network Registrar User's Guide* , Release 6.2.

Examples

The following example shows how to specify the NIS+ address of an IPv6 server:

```
nisp address 33::1
```

Related Commands

Command	Description
import nisp address	Imports the NIS+ servers option to a DHCP for IPv6 client.
nisp domain-name	Enables a server to convey a client's NIS+ domain name information to the client.

odap client

To configure On–Demand Address Pooling (ODAP) client parameters, use the **odap client** command in DHCP pool configuration mode. To remove ODAP client parameters, use the **no** form of this command.

odap client{**client-id** *id* [**interface** *type number*] [**target-server** *ip-address*]| **interface** *type number* [**client-id** *id*] [**target-server** *ip-address*]| **target-server** *ip-address* [**client-id** *id*] [**interface** *type number*]}

no odap client{**client-id** *id* [**interface** *type number*] [**target-server** *ip-address*]| **interface** *type number* [**client-id** *id*] [**target-server** *ip-address*]| **target-server** *ip-address* [**client-id** *id*] [**interface** *type number*]}

Syntax Description

client-id *id*	Configures the client ID string.
interface *type number*	(Optional) Specifies the outgoing interface for sending subnet allocation request.
target-server *ip-address*	(Optional) Configures the target ODAP server's IP address.

Command Default

The outgoing interface for sending subnet allocation request is not configured.

The Cisco IOS DHCP ODAP client module prepares the client ID to be sent in the subnet allocation request by concatenating the router hostname with the subnet pool name.

The target ODAP server's IP address is not configured.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Use the **odap client** command to configure ODAP client parameters. You must configure one of the parameters. The parameters can be specified in any order.

Examples

The following example shows how to configure ODAP client parameters:

```
Router# configure terminal
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# odap client client-id id1 interface gigabitethernet 0/0 target-server
 192.168.10.1
Eouter(dhcp-config)# end
```

Related Commands

Command	Description
odap server	Configures the ODAP server parameters.

odap server

To configure On–Demand Address Pooling (ODAP) server parameters, use the **odap server** command in DHCP pool configuration mode. To remove the ODAP server parameter settings, use the **no** form of this command.

odap server {**rebind-time** *percent-value* [**renew-time** *percent-value*]| **renew-time** *percent-value* [**rebind-time** *percent-value*]}

no odap server {**rebind-time** *percent-value* [**renew-time** *percent-value*]| **renew-time** *percent-value* [**rebind-time** *percent-value*]}

Syntax Description

rebind-time	Specifies the rebind timer.
percent-value	Percentage value of total lease.
renew-time	Specifies the renew timer.

Command Default

ODAP server parameters are not configured.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Use the **odap server** command to configure ODAP server parameters. You must specify either the rebind time or the renew time. You can specify the rebind time and renew time in any order. The rebind time cannot be less than the renew time.

Examples

The following example shows how to configure ODAP server parameters:

```
Router# configure terminal
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# odap server rebind-time 20 renew-time 10
Router(dhcp-config)# end
```

Related Commands

Command	Description
odap client	Configures ODAP client parameters.

option

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

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

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

Syntax Description

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

Command Default

The default instance number is 0.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

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

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	This command was modified. The **none** keyword was added.
15.1(3)S	This command was modified. A maximum limit of 180 characters was set for the dotted hexadecimal data and 255 characters for the ASCII data.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

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

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

The table below describes the CLI variations possible for the **hex** *hex-pattern* keyword and argument combination.

Table 1: option hex CLI Variations

Hex string format variations	CLI example	Description
Full option value as raw hex	`option 60 hex 010203`	This option has 3 bytes of data with 0x010203 hex as the content.
Bit-masked hex string	`option 60 hex 010203 mask 0000FF`	This option is the same as above except that only the first 2 bytes of data should be 0x0102.
Wild-carded hex string	`option 60 hex 010203*`	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.

option ext

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

option ext *code* {**ascii** *string*| **hex** *string*}

no option ext *code*

Syntax Description

code	Specifies the DHCP option code. The range is from 0 to 254. **Note** Only option 43 is supported under extended options. If you select any other option code, you will get a message that it is not supported.
ascii *string*	Specifies a network virtual terminal (NVT) ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
hex *string*	Specifies dotted hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.

Command Default

DHCP extended server options are not configured.

Command Modes

DHCP pool configuration (dhcp-config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.1S	This command was introduced.

Usage Guidelines

Using the **option ext** command you can specify an ASCII string upto 255 characters or 255 bytes of hexadecimal data. To do this, you need to break the string into three sets and then execute the **option ext** command three times, specifying the three strings.

```
option ext 43 ascii <first 100 characters>
option ext 43 ascii <next 100 characters>
option ext 43 ascii <last 55 characters>
```

If you want to enter 220 characters of ASCII data, you need to break the string into three, for example, two containing 100 characters each and the other containing the remaining 20 characters.

```
option ext 43 ascii <first 100 characters>
option ext 43 ascii <next 100 characters>
option ext 43 ascii <last 20 characters>
```

At any time, you can append additional characters to the string if the maximum length (255 characters or bytes) is not reached.

Only single format can be used between consecutive extended commands; that is, you cannot enter the first 100 bytes in ASCII and the next 100 bytes in hexadecimal or vice versa. Also, only one type of **option** command can be used as consecutive commands. That is, you cannot enter the **option** command and then the **option ext** command.

Use the **no option** or **no option ext** command to remove the configured option and configure the new option using the **option ext** command.

Examples

The following example shows how to configure DHCP extended option 43 and an ASCII string with 25 characters. The ASCII string of 25 characters is configured using three **option ext** commands.

```
Router(config)# ip dhcp pool pool1
Router(dhcp-config)# option ext 43 ascii 1111111111
Router(dhcp-config)# option ext 43 ascii 1111111111
Router(dhcp-config)# option ext 43 ascii 11111
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
option	Configures DHCP server options.
option hex	Enables the Cisco IOS relay agent to make forwarding decisions based on DHCP options inserted in the client-generated DHCP message.

origin

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

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

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

Syntax Description

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

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

Command Modes DHCP pool configuration

Command History

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

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

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

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

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

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

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

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

Related Commands

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

override default-router

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

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

no override default-router

Syntax Description

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

Command Default

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

Command Modes

DHCP pool secondary subnet configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
Router(config)# dhcp pool pool1
Router(config-dhcp)# network 10.1.1.1 255.255.255.248
Router(config-dhcp)# network 10.1.1.17 255.255.255.248 secondary
Router(config-dhcp-secondary-subnet)# override default-router 10.1.1.100 10.1.1.200
```

Related Commands

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

override utilization high

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

override utilization high *percentage-number*

no override utilization high *percentage-number*

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

override utilization low

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

override utilization low *percentage-number*

no override utilization low *percentage-number*

Syntax Description

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

Command Default

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

Command Modes

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

port-parameters

To configure port parameters for a Network Address Translation 64 (NAT64) mapping of addresses and ports (MAP-T) basic mapping rule, use the **port-parameters** command in NAT64 MAP-T BMR configuration mode. To remove the port parameters, use the **no** form of this command.

port-parameters share-ratio *ratio* [**start-port** *port-number*]

no port-parameters

Syntax Description

share-ratio *ratio*	Specifies the NAT64 MAP-T BMR port share ratio. Valid values for the *ratio* argument are from 1 to 4096.
start-port *port -number*	(Optional) Specifies the NAT64 MAP-T BMR starting port. Valid values for the *port-number* argument are from 1024 to 65535.

Command Default

Command Modes

NAT64 MAP-T BMR configuration (config-nat64-mapt-bmr)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

MAP-T or Mapping of address and port (MAP) double stateless translation-based solution (MAP-T) provides IPv4 hosts connectivity to and across an IPv6 domain. MAP-T builds on existing stateless IPv4/IPv6 address translation techniques that are specified in RFC 6052, RFC 6144, and RFC 6145.

Examples

The following example shows how to configure port parameters for a NAT64 MAP-T basic mapping rule:

```
Device(config)# nat64 map-t domain 89
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat4-mapt-bmr)# port-parameters share-ratio 234 start-port 2300
```

Related Commands

Command	Description
basic-mapping-rule	Configures a basic mapping rule for NAT64 MAP-T.
nat64 map-t	Configures NAT64 MAP-T settings.

preempt

To enable preemption on the redundancy group, use the **preempt**command in redundancy application group configuration mode. To disable the group's preemption, use the **no** form of this command.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Command Default

Preemption is disabled on the redundancy group.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to enable preemption on the redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) preempt
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
protocol	Defines a protocol instance in a redundancy group.

preference (DHCPv6 Guard)

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

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

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

Syntax Description

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

Command Default

No preference value is set.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

prefix-delegation

To specify a manually configured numeric prefix to be delegated to a specified client (and optionally a specified identity association for prefix delegation [IAPD] for that client), use the **prefix-delegation** command in DHCP for IPv6 pool configuration mode. To remove the prefix, use the **no** form of this command.

prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*] [*lifetime*]

no prefix-delegation *ipv6-prefix/prefix-length client-DUID* [**iaid** *iaid*]

Syntax Description

ipv6-prefix	(Optional) Specified IPv6 prefix. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
client-DUID	The DHCP unique identifier (DUID) of the client to which the prefix is delegated.
iaid *iaid*	(Optional) Identity association identifier (IAID), which uniquely identifies an IAPD on the client.

lifetime	(Optional) Sets a length of time over which the requesting router is allowed to use the prefix. The following values can be used: • **valid-lifetime** --The length of time, in seconds, that the prefix remains valid for the requesting router to use. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • **preferred-lifetime** --The length of time, in seconds, that the prefix remains preferred for the requesting router to use. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45** • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

Command Default

No manually configured prefix delegations exist.

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID. This static binding of client and prefixes can be specified based on users' subscription to an ISP using the **prefix-delegation***prefix-length* command.

The *client-DUID* argument identifies the client to which the prefix is delegated. All the configured prefixes will be assigned to the specified IAPD of the client. The IAPD to which the prefix is assigned is identified by the **iaid** argument if the **iaid** keyword is configured. If the **iaid** keyword is not configured, the prefix will be assigned to the first IAPD from the client that does not have a static binding. This function is intended to make it convenient for administrators to manually configure prefixes for a client that only sends one IAPD in case it is not easy to know the iaid in advance.

When the delegating router receives a request from a client, it checks whether there is a static binding configured for the IAPD in the client's message. If one is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

Optionally valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is between 60 and 4294967295 seconds or infinity if the **infinite** keyword is specified.

Examples

The following example configures an IAPD for a specified client:

```
prefix-delegation 2001:0DB8::/64 00030001000BBFAA2408
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

prefix-delegation aaa

To specify that prefixes are to be acquired from authorization, authentication, and accounting (AAA) servers, use the **prefix-delegation aaa**command in DHCP for IPv6 pool configuration mode. To disable this feature, use the **no** form of this command.

Cisco IOS Release 12.4(22)T and Earlier Releases and Cisco IOS Release 12.2(18)SXE, Cisco IOS XE Release 2.1, and Later Releases

prefix-delegation aaa [**method-list** *method-list* **[lifetime]** {{*valid-lifetime*| **infinite**} {*valid-lifetime*| **infinite**}| **at** {*date month year time*| *month date year time*} {*date month year time*| *month date year time*}}]

no prefix-delegation aaa method-list *method-list*

Cisco IOS Release 15.0(1)M and Later Releases

prefix-delegation aaa method-list {*method-list*| **default**} [**lifetime** {*valid-lifetime*| **infinite**} {*preferred-lifetime*| **infinite**}| **at** {*date month year time*| *month date year time*} {*date month year time*| *month date year time*}]

no prefix-delegation aaa method-list *method-list*

Syntax Description

method-list	(Optional) Indicates a method list to be defined.
method-list	Configuration type AAA authorization method list that defines how authorization will be performed.
default	Specifies the default method list, nvgened.
lifetime	(Optional) Configures prefix lifetimes.
valid-lifetime	The length of time that the prefix remains valid for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 2592000 seconds.
infinite	Indicates an unlimited lifetime.
preferred-lifetime	The length of time that the prefix remains preferred for the requesting router to use, in seconds. The range is from 60 to 4294967295. The default value is 604800 seconds.
at	Specifies absolute points in time where the prefix is no longer valid and no longer preferred.
date	The date for the valid lifetime to expire.
month	The month for the valid lifetime to expire.

year	The year for the valid lifetime to expire. The range is from 2003 to 2035.
time	The year for the valid lifetime to expire.

Command Default

The default time that the prefix remains valid is 2592000 seconds, and the default time that the prefix remains preferred for the requesting router to use is 604800 seconds.

Command Modes

DHCP for IPv6 pool configuration (config-dhcpv6)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The **default** keyword was added and the command syntax was modified to show that **lifetime** can be configured only to a **method-list**.
Cisco IOS XE Release 2.5	This command was updated. It was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

In order for the Dynamic Host Configuration Protocol (DHCP) for IPv6 server to obtain prefixes from RADIUS servers, you must also configure the AAA client and Point-to-Point Protocol (PPP) on the router. For information on how to configure the AAA client and PPP, see the "Implementing ADSL and Deploying Dial Access for IPv6" module.

Use the **aaa authorization configuration default**, **aaa group server radius**, and **radius-server host** commands to specify a named list of authorization method and RADIUS servers to contact to acquire prefixes, and then apply that named list to the **prefix-delegation aaa** command.

Valid and preferred lifetimes can be specified for the prefixes assigned from AAA servers.

The **prefix-delegation aaa** and **prefix-delegation pool** commands are mutually exclusive in a pool.

Examples

The following example shows how to specify the use of a method list named list1:

```
Router> enable
Router# configure terminal
Router(config)# ipv6 dhcp pool name
Router(config-dhcpv6)# prefix-delegation aaa method-list list1
```

Related Commands

Command	Description
aaa authorization configuration default	Downloads static route configuration information from the AAA server using TACACS+ or RADIUS.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
prefix-delegation pool	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.
radius-server host	Specifies a RADIUS server host.
sip address	Configures a SIP server IPv6 address to be returned in the SIP server's IPv6 address list option to clients.
sip domain-name	Configures an SIP server domain name to be returned in the SIP server's domain name list option to clients.

prefix-delegation pool

To specify a named IPv6 local prefix pool from which prefixes are delegated to Dynamic Host Configuration Protocol (DHCP) for IPv6 clients, use the **prefix-delegation pool**command in DHCP for IPv6 pool configuration mode. To remove a named IPv6 local prefix pool, use the **no** form of this command.

prefix-delegation pool *poolname* [**lifetime** *valid-lifetime preferred-lifetime*]

no prefix-delegation pool *poolname*

Syntax Description

poolname	User-defined name for the local prefix pool. The pool name can be a symbolic string (such as "Engineering") or an integer (such as 0).
lifetime	(Optional) Used to set a length of time for the hosts to remember router advertisements. If the optional **lifetime** keyword is configured, both valid and preferred lifetimes must be configured.
valid-lifetime	The amount of time that the prefix remains valid for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *valid-month valid-date valid-year valid-time* --A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**.

preferred-lifetime	The length of time, in seconds, that the prefix remains preferred for the requesting router to use. The following values can be used: • *seconds* --The length of time, in seconds, that the prefix remains valid for the requesting router to use. The range is from 60 through 4294967295. The *preferred-lifetime* value cannot exceed the *valid-lifetime* value. • **at** --Specifies absolute points in time where the prefix is no longer valid and no longer preferred. • **infinite** --Indicates an unlimited lifetime. • *preferred-month preferred-date preferred-year preferred-time*-- A fixed duration of time for hosts to remember router advertisements. The format to be used can be **oct 24 2003 11:45** or **24 oct 2003 11:45**

Command Default

No IPv6 local prefix pool is specified. Valid lifetime is 2592000 seconds (30 days). Preferred lifetime is 604800 seconds (7 days).

Command Modes

DHCP for IPv6 pool configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The **prefix-delegation pool**command specifies a named IPv6 local prefix pool from which prefixes are delegated to clients. Use the **ipv6 local pool** command to configure the named IPv6 prefix pool.

Optionally, valid and preferred lifetimes can be specified for the prefixes assigned from this pool. Users should coordinate the specified lifetimes with the lifetimes on prefixes from the upstream delegating router if the prefixes were acquired from that router.

The **lifetime**keyword can be specified in one of two ways:

- A fixed duration that stays the same in consecutive advertisements.
- Absolute expiration time in the future so that advertised lifetime decrements in real time, which will result in a lifetime of 0 at the specified time in the future.

The specified length of time is from 60 to 4,294,967,295 seconds or infinity if the **infinite** keyword is specified.

The Cisco IOS DHCP for IPv6 server can assign prefixes dynamically from an IPv6 local prefix pool, which is configured using the **ipv6 local pool** command and associated with a DHCP for IPv6 configuration pool

using the **prefix-delegation pool** command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes, if any, from the pool.

After the client releases the previously assigned prefixes, the server will return the prefixes to the pool for reassignment to other clients.

Examples

The following example specifies that prefix requests should be satisfied from the pool called client-prefix-pool. The prefixes should be delegated with the valid lifetime set to 1800 seconds, and the preferred lifetime is set to 600 seconds:

```
prefix-delegation pool client-prefix-pool lifetime 1800 600
```

Related Commands

Command	Description
ipv6 dhcp pool	Configures a DHCP for IPv6 pool and enters DHCP for IPv6 pool configuration mode.
ipv6 local pool	Configures a local IPv6 prefix pool.
prefix-delegation	Specifies a manually configured numeric prefix that is to be delegated to a particular client's IAPD.
show ipv6 dhcp pool	Displays DHCP for IPv6 configuration pool information.

priority (firewall)

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode. To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]

no priority *value* [**failover-threshold** *value*]

Syntax Description

value	The priority value. The range is from 1 to 255.
failover-threshold *value*	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The priority of the redundancy group is used to determine a redundancy group's active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

Command	Description
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

protocol

To define a protocol instance in a redundancy group, use the **protocol**command in redundancy application configuration mode. To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*

no protocol *id*

Syntax Description

id	Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.

Command	Description
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

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

interface-type	Interface type. For more information, use the question mark (?) online help function.
number	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 information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM RBE 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 loopback 0
```

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.

redundancy

To enter redundancy configuration mode, use the **redundancy**command in global configuration mode. This command does not have a **no** form.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.

Release	Modification
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
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(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.
12.2(33) SRE	This command was modified. The interchassis subconfiguration mode was added.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.

- Define the peer monitoring method using the **monitor** command.

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

Examples

The following example shows how to enable redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Examples

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

Examples

The following example shows how to enter the main CPU submode:

```
Router(config)#
redundancy
Router(config-r)#
main-cpu
Router(config-r-mc)#
```

Examples

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
```

```
Router(config)# redundancy

Router(config-r)# ?

Redundancy configuration commands:
  associate  Associate redundant slots
  exit       Exit from redundancy configuration mode
  main-cpu   Enter main-cpu mode
  no         Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?
Redundancy configuration commands:
  default         Set a command to its defaults
  exit            Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu        Enter main-cpu mode
  mode            redundancy mode for this chassis
  no              Negate a command or set its defaults
  policy          redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?

Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults
Router(config-r)# interchassis group 100

R1(config-r-ic)# ?
Interchassis redundancy configuration commands:
  backbone  specify a backbone interface for the redundancy group
  exit      Exit from interchassis configuration mode
  member    specify a redundancy group member
  mlacp     mLACP interchassis redundancy group subcommands
  monitor   define the peer monitoring method
  no        Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.

Command	Description
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers.

redundancy asymmetric-routing enable

To establish an asymmetric flow diversion tunnel for each redundancy group, use the **redundancy asymmetric-routing enable** command in interface configuration mode. To remove the established flow diversion tunnel, use the **no** form of this command.

redundancy asymmetric-routing enable

no redundancy asymmetric-routing enable

Syntax Description

This command has no arguments or keywords.

Command Default

An asymmetric routing traffic diversion tunnel is not configured for redundancy groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

You must configure this command on a traffic interface that sends or receives asymmetric routing traffic. A tunnel is established between the traffic interface and the asymmetric routing interface for each redundancy group.

Examples

The following example shows how to enable redundancy group asymmetric routing on a Gigabit Ethernet interface:

```
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# redundancy asymmetric-routing enable
```

Related Commands

Command	Description
asymmetric-routing	Sets up an asymmetric routing link interface and enables applications to divert packets received on the standby redundancy group to the active.
interface	Configures an interface and enters interface configuration mode.

redundancy group

To configure fault tolerance for the mobile router, use the **redundancy group** command in mobile router configuration mode. To disable this functionality, use the **no** form of this command.

redundancy group *name*

no redundancy group *name*

Syntax Description

name	Name of the mobile router group.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Usage Guidelines

The **redundancy group** command provides f ault tolerance by selecting one mobile router in the redundancy group *name* argument to provide connectivity for the mobile networks. This mobile router is in the active state. The other mobile routers are passive and wait until the active mobile router fails before a new active mobile router is selected. Only the active mobile router registers and sets up proper routing for the mobile networks. The redundancy state is either active or passive.

Examples

The following example selects the mobile router in the sanjose group, to provide fault tolerance:

```
ip mobile router
 redundancy group sanjose
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
standby name	Configures the name of the standby group, which is associated with the mobile router.

redundancy group (interface)

To enable the redundancy group (RG) traffic interface configuration, use the **redundancy group** command in interface configuration mode. To remove the redundancy group traffic interface configuration, use the **no** form of this command.

redundancy group *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}| **autoconfig**} [**exclusive**] [**decrement** *value*]

no redundancy group *id* {**ip**| **ipv6** {*link-local-address* | *ipv6-address*/*prefix-length*}}

Syntax Description

id	Redundancy group ID. Valid values are from 1 and 2.
ip *virtual-ip*	Enables IPv4 RGs and sets a virtual IPv4 address.
ipv6	Enables IPv6 RGs.
link-local-address	Link local address.
ipv6-address/*prefix-length*	IPv6 address and the length of the IPv6 prefix. IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
autoconfig	Obtains IP addresses through autoconfiguration.
exclusive	(Optional) Specifies whether the interface is exclusive to an RG.
decrement *number*	(Optional) Specifies the number that is decremented from the priority when the state of an interface goes down. The configured decrement value overrides the default number that is configured for an RG. Valid values are from 1 to 255.

Command Default

Redundancy group traffic interface configuration is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. The *virtual-ip*, *link-local-address*, *ipv6-address*/*prefix-length* arguments and **ip**, **ipv6**, and **autoconfig** keywords were added.

Usage Guidelines

Use this command to configure a redundancy group for stateful switchover.

The virtual IP address and the physical address must be in the same subnet.

When autoconfiguration is enabled, the interface obtains an IP address automatically.

Examples

The following example shows how to enable the IPv6 redundancy group traffic interface configuration:

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# redundancy group 2 ipv6 FE80::260:3EFF:FE11:6770 exclusive
```

Related Commands

Command	Description
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
interface	Configures an interface and enters interface configuration mode.
name	Configures the name of a redundancy group.
preempt	Enables preemption on a redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures an RII for a redundancy group.

relay agent information

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

relay agent information

no relay agent information

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

DHCP class configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 000000000000000000000FF
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 *vrf-name* 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.
ip-address	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Command Default

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.

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 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

ip-address	IPv4 address of DHCP server from which the DHCP client packets are relayed.
subnet-mask	Subnet mask that matches the subnet of the incoming interface of the DHCP client packet.

Command Default

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.

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 *vrf-name* 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.
ip-address	IPv4 address of the remote DHCP server to which the DHCP client packets are relayed.

Command Default

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.

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.

relay-information hex

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

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

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

Syntax Description

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

Command Default

No default behavior or values

Command Modes

Relay agent information option configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 000000000000000000000000FF
ip dhcp class CLASS2
 relay agent information
```

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

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	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.

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.

Command	Description
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.
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.

remote command

To execute a Cisco 7600 series router command directly on the switch console or a specified module without having to log into the Cisco 7600 series router first, use the **remote command** command in privileged EXEC mode.

remote command {**module** *num*| **standby-rp**| **switch**} *command*

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.
command	Command to be executed.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	The **standby-rp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote command switch** command, the prompt changes to Switch-sp#.

This command is supported on DFC-equipped modules and the supervisor engine only.

This command does not support command completion, but you can use shortened forms of the command (for example, entering **sh** for **show**).

Examples

This example shows how to execute the **show calendar** command from the standby route processor:

```
Router#
remote command standby-rp show calendar
Switch-sp#
09:52:50 UTC Mon Nov 12 2001
Router#
```

Related Commands

Command	Description
remote login	Accesses the Cisco 7600 series router console or a specific module.

remote login

To access the Cisco 7600 router console or a specific module, use the **remote login** command in privileged EXEC mode.

remote login {**module** *num*| **standby-rp**| **switch**}

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(140SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to include the **standby-rp** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelin

Caution When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote login module** *num* command, the prompt changes to Router-dfcx# or Switch-sp#, depending on the type of module to which you are connecting.

When you execute the **remote login standby-rp** command, the prompt changes to Router-sdby#.

When you execute the **remote login switch** command, the prompt changes to Switch-sp#.

The **remote login module** *num* command is identical to the **attach** command.

There are two ways to end the session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit
[Connection to Switch closed by foreign host]
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the Cisco 7600 series router processor:

```
Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

Related Commands

Command	Description
attach	Connects to a specific module from a remote location.

remote-ip (IPC transport-SCTP remote)

To define at least one IP address of the redundant peer that is used to communicate with the local device, use the **remote-ip**command in IPC transport-SCTP remote configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

remote-ip *peer-real-ip-address* [*peer-real-ip-address2*]

no remote-ip *peer-real-ip-address* [*peer-real-ip-address2*]

Syntax Description

peer-real-ip-address	IP address of the remote peer. The remote IP addresses must match the local IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
peer-real-ip-address2	(Optional) IP address of the remote peer.

Command Default

No IP addresses are defined.

Command Modes

IPC transport-SCTP remote configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **remote-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switch Over (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
redundancy inter-device
 scheme standby HA-in
!
ipc zone default
 association 1
```

```
no shutdown
protocol sctp
 local-port 5000
  local-ip 10.0.0.1
 remote-port 5000
  remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

remote-port

To define the remote Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **remote-port**command in SCTP protocol configuration mode.

remote-port *remote-port-number*

Syntax Description

remote-port-number	Remote port number, which should be the same as the local port number on the peer router (which is specified via the **local-port** command).

Command Default

A remote SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **remote-port** command enters IPC transport-SCTP remote configuration mode, which allows you to specify at least one remote IP address (via the **remote-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
redundancy inter-device
 scheme standby HA-in
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port that is used to communicate with the redundant peer.

Command	Description
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.

remote-span

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

remote-span

no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported in the VLAN database mode.

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

Examples

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

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

This example shows how to remove the RSPAN designation:

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

Related Commands

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

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 Cisco IOS Release 12.2SXH

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
```

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

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	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.

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.

Command	Description
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.
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.