

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

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

Defaults

1 day

Command Modes

DHCP pool configuration

Command History

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

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

<i>device-real-ip-address</i>	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 Routing and Forwarding (VRF). A virtual IP (VIP) address cannot be used.
<i>device-real-ip-address2</i>	(Optional) IP address of the local device.

Defaults

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
```

■ local-ip (IPC transport-SCTP local)

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

<i>local-port-number</i>	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).
--------------------------	---

Defaults

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

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 address 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 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.

manager (DFP agent)

This command has been replaced by the following commands:

- **inservice (DFP agent)**
- **interval (DFP agent)**
- ip dfp agent
- **password (DFP agent)**
- **port (DFP agent)**

maxconns (server farm)

To limit the number of active connections to the real server, use the **maxconns** command in SLB server farm configuration mode. To restore the default of 4294967295, use the **no** form of this command.

maxconns *maximum-number* [**sticky-override**]

no maxconns

Syntax Description		
<i>maximum-number</i>		Maximum number of simultaneous active connections on the real server. Valid values range from 1 to 4294967295. The default is 4294967295.
sticky-override		(Optional) Allow sticky load balancing to exceed <i>maximum-number</i> for this real server.

Defaults The default maximum number of simultaneous active connections on the real server is 4294967295.

Command Modes SLB server farm configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
	12.2	This command was integrated into Cisco IOS Release 12.2.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.1(18)E	The sticky-override keyword was added.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples The following example limits the real server to a maximum of 1000 simultaneous active connections:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# maxconns 1000
```

Related Commands	Command	Description
	real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
	show ip slb reals	Displays information about the real servers.
	show ip slb severfarms	Displays information about the server farm configuration.

nat

To configure IOS SLB Network Address Translation (NAT) and specify a NAT mode, use the **nat** SLB server farm configuration command. To remove a NAT configuration, use the **no** form of this command.

nat server

no nat server

Syntax Description	server	Specifies that the destination address in load-balanced packets sent to the real server is the address of the real server chosen by the server farm load-balancing algorithm.
---------------------------	---------------	---

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

Command Modes	SLB server farm configuration
----------------------	-------------------------------

Command History	Release	Modification
	12.1(1)E	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines	The no nat command is allowed only if the virtual server was removed from service with the no inservice command.
-------------------------	--

Examples The following example changes to IOS SLB server farm configuration mode and configures NAT mode as server address translation on the server farm named FARM2:

```
ip slb serverfarm FARM2
 nat server
```

Related Commands	Command	Description
	ip slb serverfarm	Associates a real server farm with a virtual server.
	real	Identifies a real server as a member of a server farm.
	show ip slb serverfarms	Displays information about the server farm configuration.

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

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

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

netbios-node-type

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

netbios-node-type *type*

no netbios-node-type

Syntax Description

<i>type</i>	Specifies the NetBIOS node type. Valid types are: <ul style="list-style-type: none"> • b-node—Broadcast • p-node—Peer-to-peer • m-node—Mixed • h-node—Hybrid (recommended)
-------------	--

Command Modes

DHCP pool configuration

Command History

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

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

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

```
no network
```

Syntax Description

<i>network-number</i>	The IP address of the DHCP address pool.
<i>mask</i>	(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.
<i>prefix-length</i>	(Optional) The number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

This command is valid for DHCP subnetwork address pools only. If the mask or prefix length is not specified, the class A, B, or C natural mask is used. 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** command.

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

Examples

The following example configures 172.16.0.0/16 as the subnetwork number and mask of the DHCP pool:

```
network 172.16.0.0/16
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.

Command	Description
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.

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

<i>address</i>	Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server. One IP address is required, although you can specify up to eight addresses in one command line.
<i>address2...address8</i>	(Optional) Specifies up to eight addresses in the command line.

Defaults

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

Command Modes

DHCP pool configuration

Command History

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

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.

no ip gratuitous-arps

To disable the transmission of gratuitous Address Resolution Protocol (ARP) messages for an address in a local pool, use the **no ip gratuitous-arps** command in global configuration mode.

no ip gratuitous-arps

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines A Cisco router will send out a gratuitous ARP message when a client connects and negotiates an address over a PPP connection. This transmission occurs even when the client receives the address from a local address pool.

Examples The following example disables gratuitous arp messages from being sent:

```
no ip gratuitous-arps
```

object (tracking)

To specify an object for a tracked list, use the **object** command in tracking configuration mode. To remove the object from the tracked list, use the **no** form of this command.

```
object object-number [not] [weight weight-number]
```

```
no object object-number [not] [weight weight-number]
```

Syntax Description	
<i>object-number</i>	Object in a tracked list of objects. Range is from 1 to 500.
not	(Optional) Negates the state of an object.
	Note The not keyword cannot be used in a weight or percentage threshold list only the Boolean list.
weight <i>weight-number</i>	The optional weight keyword specifies a threshold weight for each object.

Defaults The object is removed from the tracked list.

Command Modes Tracking configuration

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

Examples The following example shows two serial interfaces (objects) that are in tracked list 100. The Boolean “not” negates state of object 2 , which means when object 2 is up, the tracked list regards the object as down.

```
track 1 interface serial2/0 line-protocol
track 2 interface serial2/1 line-protocol
```

```
track 100 list boolean and
  object 1
  object 2 not
```

Related Commands	Command	Description
	show track	Displays tracking information.
	track list threshold percentage	Tracks a list of objects as to the up and down object states using a threshold percentage.
	track list threshold weight	Tracks a list of objects as to the up and down object states using a threshold weight.
	threshold weight	Specifies a threshold weight for a tracked list.

option

To configure Cisco IOS Dynamic Host Configuration Protocol (DHCP) server options, use the **option** command in DHCP pool configuration mode. To remove the options, use the **no** form of this command.

```
option code [instance number] {ascii string | hex string | ip address}
```

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

Syntax Description

<i>code</i>	Specifies the DHCP option code.
instance <i>number</i>	(Optional) Specifies a number from 0 to 255.
ascii <i>string</i>	Specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
hex <i>string</i>	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.
ip <i>address</i>	Specifies an IP address.

Defaults

The default instance number is 0.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

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

Examples

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

```
option 19 hex 01
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
option 72 ip 172.16.3.252 172.16.3.253
```

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

origin

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

```
origin { dhcp | aaa | ipcp | file url } [subnet size initial size [autogrow size]]
```

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

Syntax Description

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

Defaults

The default size value is /0.

Command Modes

DHCP pool configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

Command	Description
<code>show ip dhcp pool</code>	Displays information about the DHCP address pools.

password (DFP agent)

To configure a DFP agent password for MD5 authentication, use the **password** command in DFP agent configuration mode. To remove the DFP agent password, use the **no** form of this command.

password [**0** | **7**] *password* [*timeout*]

no password

Syntax Description		
	0	(Optional) Unencrypted password. This is the default setting.
	7	(Optional) Encrypted password.
	<i>password</i>	(Optional) Password value for MD5 authentication. Note This password must match the password configured on the host agent.
	<i>timeout</i>	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted. The valid range is from 0 to 65535. The default is 180.

Defaults No password is enabled.

Command Modes DFP agent configuration

Command History	Release	Modification
	12.1(8a)E	This command was introduced.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines The timeout option allows you to change the password without stopping messages between the DFP agent and its manager. The default value is 180 seconds.

During the timeout, the agent sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After the timeout expires, the agent sends and receives packets only with the new password; received packets that use the old password are discarded.

If you are changing the password for an entire load-balanced environment, set a longer timeout. This allows enough time for you to update the password on all agents and servers before the timeout expires. It also prevents mismatches between agents and servers that have begun running the new password and agents, and servers on which you have not yet changed the old password.

Examples The following example shows how to set the DFP agent password (unencrypted by default) to Cookies and the timeout to 360 seconds:

```
Router(config)# ip dfp agent slb
```

```
Router(config-dfp)# password Cookies 360
```

Related Commands

Command	Description
agent	Identifies a DFP agent to which IOS SLB can connect.
ip dfp agent	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
ip slb dfp	Configures DFP, supplies an optional password, and initiates DFP configuration mode.
replicate casa (firewall farm)	Configures a stateful backup of IOS SLB decision tables to a backup switch.
replicate casa (virtual server)	Configures a stateful backup of IOS SLB decision tables to a backup switch.

permit (IP)

To set conditions to allow a packet to pass a named IP access list, use the **permit** command in access list configuration mode. To remove a permit condition from an access list, use the **no** form of this command.

```
[sequence-number] permit source [source-wildcard]
```

```
[sequence-number] permit protocol source source-wildcard destination destination-wildcard  
[option option-name] [precedence precedence] [tos tos] [log] [time-range time-range-name]  
[fragments]
```

```
no sequence-number
```

```
no permit source [source-wildcard]
```

```
no permit protocol source source-wildcard destination destination-wildcard [option option-name]  
[precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]
```

Internet Control Message Protocol (ICMP)

```
[sequence-number] permit icmp source source-wildcard destination destination-wildcard  
[icmp-type [icmp-code] | icmp-message] [precedence precedence] [tos tos] [log] [time-range  
time-range-name] [fragments]
```

Internet Group Management Protocol (IGMP)


```
[sequence-number] permit igmp source source-wildcard destination destination-wildcard  
[igmp-type] [precedence precedence] [tos tos] [log] [time-range time-range-name]  
[fragments]
```

Transmission Control Protocol (TCP)

```
[sequence-number] permit tcp source source-wildcard [operator [port]] destination  
destination-wildcard [operator [port]] [established | {match-any | match-all} {+ | -}  
flag-name] [precedence precedence] [tos tos] [log] [time-range time-range-name]  
[fragments]
```

User Datagram Protocol (UDP)

```
[sequence-number] permit udp source source-wildcard [operator [port]] destination  
destination-wildcard [operator [port]] [precedence precedence] [tos tos] [log] [time-range  
time-range-name] [fragments]
```

Syntax Description	
<i>sequence-number</i>	(Optional) Sequence number assigned to the permit statement. The sequence number causes the system to insert the statement in that numbered position in the access list.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> Use a 32-bit quantity in four-part dotted-decimal format. Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>protocol</i>	Name or number of an Internet protocol. The <i>protocol</i> argument can be one of the keywords eigrp , gre , icmp , igmp , ip , ipinip , nos , ospf , tcp , or udp , or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the ip keyword.
	 <p>Note When the icmp, igmp, tcp, and udp keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the permit command.</p>
icmp	Permits only ICMP packets. When you enter the icmp keyword, you must use the specific command syntax shown for the ICMP form of the permit command.
igmp	Permits only IGMP packets. When you enter the igmp keyword, you must use the specific command syntax shown for the IGMP form of the permit command.
tcp	Permits only TCP packets. When you enter the tcp keyword, you must use the specific command syntax shown for the TCP form of the permit command.
udp	Permits only UDP packets. When you enter the udp keyword, you must use the specific command syntax shown for the UDP form of the permit command.

<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted-decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the any keyword as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
option <i>option-name</i>	(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255, or by the corresponding IP Option name, as listed in Table 3 in the “Usage Guidelines” section.
precedence <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.
tos <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the “Usage Guidelines” section of the access-list (IP extended) command.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the logging console command.)
time-range <i>time-range-name</i>	(Optional) Name of the time range that applies to this permit statement. The name of the time range and its restrictions are specified by the time-range and absolute or periodic commands, respectively.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the fragments keyword, see the “ Access List Processing of Fragments ” and “ Fragments and Policy Routing ” sections in the “Usage Guidelines” section.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the “Usage Guidelines” section of the access-list (IP extended) command.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the access-list (IP extended) command.

<i>operator</i>	<p>(Optional) Compares source or destination ports. Operators include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i> arguments, it must match the source port. If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i> arguments, it must match the destination port.</p> <p>The range operator requires two port numbers. Up to ten port numbers can be entered for the eq (equal) and neq (not equal) operators. All other operators require one port number.</p>
<i>port</i>	<p>(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the access-list (IP extended) command.</p> <p>TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.</p>
established	<p>(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection.</p> <p>Note The established keyword can be used only with the old command-line interface (CLI) format. To use the new CLI format, you must use the match-any or match-all keywords followed by the + or - keywords and <i>flag-name</i> argument.</p>
{ match-any match-all }	<p>(Optional) For the TCP protocol only: A match occurs if the TCP datagram has certain TCP flags set or not set. You use the match-any keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the match-all keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the match-any and match-all keywords with the + or - keyword and the <i>flag-name</i> argument to match on one or more TCP flags.</p>
{+ -} <i>flag-name</i>	<p>(Optional) For the TCP protocol only: The + keyword matches IP packets if their TCP headers contain the TCP flags that are specified by the <i>flag-name</i> argument. The - keyword matches IP packets that do not contain the TCP flags specified by the <i>flag-name</i> argument. You must follow the + and - keywords with the <i>flag-name</i> argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: urg, ack, psh, rst, syn, and fin.</p>

Syntax Description

There are no specific conditions under which a packet passes the named access list.

Command Modes

Access list configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(1)T	The time-range <i>time-range-name</i> keyword and argument were added.
	12.0(11)	The fragments keyword was added.
	12.2(13)T	The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
	12.2(14)S	The <i>sequence-number</i> argument was added.
	12.2(15)T	The <i>sequence-number</i> argument was integrated into Cisco IOS Release 12.2(15)T.
	12.3(4)T	The option <i>option-name</i> keyword and argument were added. The match-any , match-all , + and - keywords and the <i>flag-name</i> argument were added.
	12.3(7)T	Command functionality was modified to allow up to ten port numbers to be added after the eq and neq operators so that an access list entry can be created with noncontiguous ports.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **permit** statement is in effect.

log Keyword

A log message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute-interval). See the **ip access-list log-update** command for more information.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

If you enable Cisco Express Forwarding (CEF) and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF-switched. They are fast-switched. Logging disables CEF.

Access List Filtering of IP Options

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from their URL: www.iana.org.

Cisco IOS software allows you to filter packets according to whether they contain one or more of the legitimate IP Options by entering either the IP Option value or the corresponding name for the *option-name* argument as shown in [Table 3](#).

Table 3 IP Option Values and Names

IP Option Value or Name	Description
0 to 255	IP Options values.
add-ext	Match packets with Address Extension Option (147).
any-options	Match packets with any IP Option.
com-security	Match packets with Commercial Security Option (134).
dps	Match packets with Dynamic Packet State Option (151).
encode	Match packets with Encode Option (15).
eool	Match packets with End of Options (0).
ext-ip	Match packets with Extended IP Options (145).
ext-security	Match packets with Extended Security Option (133).
finn	Match packets with Experimental Flow Control Option (205).
imitd	Match packets with IMI Traffic Descriptor Option (144).
lsr	Match packets with Loose Source Route Option (131).
mtup	Match packets with MTU Probe Option (11).
mtur	Match packets with MTU Reply Option (12).
no-op	Match packets with the No Operation Option (1).
nsapa	Match packets with the NSAP Addresses Option (150).
record-route	Match packets with Router Record Route Option (7).
router-alert	Match packets with Router Alert Option (148).
sdb	Match packets with Selective Directed Broadcast Option (149).
security	Match packets with Base Security Option (130).
ssr	Match packets with Strict Source Routing Option (137).
stream-id	Match packets with Stream ID Option (136).
timestamp	Match packets with Time Stamp Option (68).
traceroute	Match packets with Trace Route Option (82).
ump	Match packets with Upstream Multicast Packet Option (152).
visa	Match packets with Experimental Access Control Option (142).
zsu	Match packets with Experimental Measurement Option (10).

Filtering IP Packets Based on TCP Flags

The access list entries that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have very specific groups of TCP flags set or not set. Users can select any desired combination of TCP flags with which to filter TCP packets. Users can configure access list entries in order to allow matching on a flag that is set and on a flag that is not set. Use the +

and - keywords with a flag name to specify that a match is made based on whether a TCP header flag has been set. Use the **match-any** and **match-all** keywords to allow the packet if any or all, respectively, of the flags specified by the + or - keyword and *flag-name* argument have been set or not set.

Access List Processing of Fragments

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

If the Access-List Entry Has...	Then...
...no fragments keyword (the default behavior), and assuming all of the access-list entry information matches,	<p>For an access list entry that contains only Layer 3 information:</p> <ul style="list-style-type: none"> The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. <p>For an access list entry that contains Layer 3 and Layer 4 information:</p> <ul style="list-style-type: none"> The entry is applied to nonfragmented packets and initial fragments. <ul style="list-style-type: none"> If the entry is a permit statement, then the packet or fragment is permitted. If the entry is a deny statement, then the packet or fragment is denied. The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and <ul style="list-style-type: none"> If the entry is a permit statement, then the noninitial fragment is permitted. If the entry is a deny statement, then the next access list entry is processed. <p>Note The deny statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.</p>
...the fragments keyword, and assuming all of the access list entry information matches,	The access list entry is applied only to noninitial fragments. The fragments keyword cannot be configured for an access list entry that contains any Layer 4 information.

Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments** keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are

multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

**Note**

The **fragments** keyword cannot solve all cases that involve access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list has entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy-routed, even if the first fragment is not policy-routed.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made, and it is more likely that policy routing will occur as intended.

Creating an Access List Entry with Noncontiguous Ports

For Cisco IOS Release 12.3(7)T and later releases, you can specify noncontiguous ports on the same access control entry, which greatly reduces the number of access list entries required for the same source address, destination address, and protocol. If you maintain large numbers of access list entries, we recommend that you consolidate them when possible by using noncontiguous ports. You can specify up to ten port numbers following the **eq** and **neq** operators.

Examples

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
deny 192.168.34.0 0.0.0.255
permit 172.16.0.0 0.0.255.255
permit 10.0.0.0 0.255.255.255
! (Note: all other access implicitly denied).
```

The following example permits Telnet traffic on Mondays, Tuesdays, and Fridays from 9:00 a.m. to 5:00 p.m.:

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
```

interface ethernet 0

```
ip access-group legal in
```

The following example sets a permit condition for an extended access list named filter2. The access list entry specifies that a packet may pass the named access list only if it contains the NSAP Addresses IP Option, which is represented by the IP Option value nsapa.

```
Router(config)# ip access-list extended filter2
Router(config-ext-nacl)# permit ip any any option nsapa
```

The following example sets a permit condition for an extended access list named `kmdfilter1`. The access list entry specifies that a packet can pass the named access list only if the RST IP flag has been set for that packet:

```
Router(config)# ip access-list extended kmdfilter1
Router(config-std-nacl)# permit tcp any any match-any +rst
```

The following example sets a permit condition for an extended access list named `kmdfilter1`. The access list entry specifies that a packet can pass the named access list only if the RST and FIN TCP flags have been set for that packet:

```
Router(config)# ip access-list extended kmdfilter1
Router(config-std-nacl)# permit tcp any any match-any +rst +fin
```

The following example shows how to add an entry to an existing access list:

```
Router# show access-lists

Standard IP access list 1
 2 permit 10.0.0.0, wildcard bits 0.0.255.255
 5 permit 10.0.0.0, wildcard bits 0.0.255.255
10 permit 10.0.0.0, wildcard bits 0.0.255.255
20 permit 10.0.0.0, wildcard bits 0.0.255.255

Router(config)# ip access-list standard 1
Router(config-std-nacl)# 15 permit 10.0.0.0 0.0.255.255
```

The following examples shows how the entry with the sequence number of 20 is removed from the access list:

```
Router(config)# ip access-list standard 1
Router(config-std-nacl)# no 20
```

```
Router# show access-lists

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.4.0.0, wildcard bits 0.0.0.255
```

The following examples shows how, if a user tries to enter an entry that is a duplicate of an entry already on the list, no changes occur. The entry that the user is trying to add is a duplicate of the entry already in the access list with a sequence number of 20.

```
Router# show access-lists 101

Extended IP access list 101
 10 permit ip host 10.0.0.0 host 10.5.5.34
 20 permit icmp any any
 30 permit ip host 10.0.0.0 host 10.2.54.2
 40 permit ip host 10.0.0.0 host 10.3.32.3 log

Router(config)# ip access-list extended 101
Router(config-ext-nacl)# 100 permit icmp any any
Router(config-ext-nacl)# end

Router# show access-lists 101

Extended IP access list 101
 10 permit ip host 10.3.3.3 host 10.5.5.34
 20 permit icmp any any
 30 permit ip host 10.34.2.2 host 10.2.54.2
 40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

The following example shows what occurs if a user tries to enter a new entry with a sequence number of 20 when an entry with a sequence number of 20 is already in the list. An error message appears, and no change is made to the access list.

```
Router# show access-lists 101

Extended IP access lists 101
 10 permit ip host 10.3.3.3 host 10.5.5.34
 20 permit icmp any any
 30 permit ip host 10.34.2.2 host 10.2.54.2
 40 permit ip host 10.3.4.31 host 10.3.32.3 log

Router(config)# ip access-lists extended 101
Router(config-ext-nacl)# 20 permit udp host 10.1.1.1 host 10.2.2.2

Duplicate sequence number.

Router(config-ext-nacl)# end

Router# show access-lists 101

Extended IP access lists 101
 10 permit ip host 10.3.3.3 host 10.5.5.34
 20 permit icmp any any
 30 permit ip host 10.34.2.2 host 10.2.54.2
 40 permit ip host 10.3.4.31 host 10.3.32.3 log
```

The following example shows several **permit** statements that can be consolidated into one access list entry with noncontiguous ports. The **show access-lists** command is entered to display a group of access list entries for the access list named aaa.

```
Router# show access-lists aaa

Extended IP access lists aaa
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

Because the entries are all for the same **permit** statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
Router# configure terminal
Router(config)# ip access-list extended aaa
Router(config-ext-nacl)# no 10
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# no 30
Router(config-ext-nacl)# no 40
Router(config-ext-nacl)# permit tcp any eq telnet ftp any eq 450 679
Router(config-ext-nacl)# end
```

The following example shows the creation of the consolidated access list entry:

```
Router# show access-lists aaa

Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 450 679
```

Related Commands

Command	Description
absolute	Specifies an absolute time when a time range is in effect.
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
ip access-group	Controls access to an interface.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
ip access-list resequence	Applies sequence numbers to the access list entries in an access list.
ip options	Drops or ignores IP Options packets that are sent to the router.
logging console	Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
show access-lists	Displays a group of access-list entries.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

port (DFP agent)

To define the port number to be used by the DFP manager to connect to the DFP agent, use the **port** command in DFP agent configuration mode. To disable the port number definition and remove existing connections, use the **no** form of this command.

port *port-number*

no port *port-number*

Syntax Description	<i>port-number</i>	Port number used by a DFP manager to connect to a DFP agent. The valid range is from 1 to 65535.
---------------------------	--------------------	--

Defaults	No port number is defined.
-----------------	----------------------------

Command Modes	DFP agent configuration
----------------------	-------------------------

Command History	Release	Modification
	12.1(8a)E	This command was introduced.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Examples In the following example, the DFP manager is enabled and will connect to the DFP agent using port number 2221:

```
Router(config)# ip dfp agent slb
Router(config-dfp)# port 2221
```

Related Commands	Command	Description
	agent	Identifies a DFP agent to which IOS SLB can connect.
	ip dfp agent	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
	ip slb dfp	Configures DFP, supplies an optional password, and initiates DFP configuration mode.

predictor

To specify the load-balancing algorithm for selecting a real server in the server farm, use the **predictor** command in SLB server farm configuration mode. To restore the default load-balancing algorithm of weighted round robin, use the **no** form of this command.

predictor [**roundrobin** | **leastconns**]

no predictor

Syntax Description

roundrobin	(Optional) Use the weighted round robin algorithm for selecting the real server to handle the next new connection for the server farm.
leastconns	(Optional) Use the weighted least connections algorithm for selecting the real server to handle the next new connection for this server farm.

Defaults

The default predictor is weighted round robin.

Command Modes

SLB server farm configuration

Command History

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

Examples

The following example specifies the weighted least connections algorithm:

```
ip slb serverfarm PUBLIC
predictor leastconns
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farm configuration.
weight	Specifies the capacity of the real server, relative to other real servers in the server farm.

real

To identify a real server as a member of a server farm, use the **real** command in SLB server farm configuration mode. To remove the real server from the IOS SLB configuration, use the **no** form of this command.

real *ip-address*

no real *ip-address*

Syntax Description	<i>ip-address</i>	Real server IP address.
---------------------------	-------------------	-------------------------

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

Command Modes	SLB server farm configuration
----------------------	-------------------------------

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

Examples The following example identifies a real server as a member of the server farm:

```
ip slb serverfarm PUBLIC
 real 10.1.1.1
```

Related Commands	Command	Description
	inservice (real server)	Enables the real server for use by IOS SLB.
	show ip slb serverfarms	Displays information about the server farm configuration.
	show ip slb reals	Displays information about the real servers.

reassign

To specify the threshold of consecutive unanswered synchronizations that, if exceeded, results in an attempted connection to a different real server, use the **reassign** command in SLB real server configuration mode. To restore the default reassignment threshold, use the **no** form of this command.

reassign *threshold*

no reassign

Syntax Description

<i>threshold</i>	Number of unanswered TCP SYNs that are directed to a real server before the connection is reassigned to a different real server. An unanswered SYN is one for which no SYN or ACK is detected before the next SYN arrives from the client. IOS SLB allows 30 seconds for the connection to be established or for a new SYN to be received. If neither of these events occurs within that time, the connection is removed from the IOS SLB database. The 30-second timer is restarted for each SYN as long as the number of connection reassignments specified on the faildetect command's numconns keyword is not exceeded. See the faildetect command for more information. Valid threshold values range from 1 to 4 SYNs. The default value is 3.
------------------	--

Defaults

The default threshold is three SYNs.

Command Modes

SLB real server configuration

Command History

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

Examples

The following example sets the threshold of unanswered SYNs to 2:

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 reassign 2
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

relay agent information

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

relay agent information

no relay agent information

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes DHCP class configuration

Command History	Release	Modification
	12.2(13)ZH	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines If this command is omitted for DHCP class-based address allocation, then the DHCP class matches to any relay agent information option, whether it is present or not.

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

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

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

ip dhcp class CLASS2
  relay agent information
```

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

relay destination

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

Defaults

No 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.

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 SG.

Examples

In the following example, multiple relay sources and destinations may be configured for a relay pool. This is similar the ip helper-address configuration on multiple interfaces. Pools are matched to the (possibly multiple) IP addresses on an incoming interface in the order in which they appear when using the **show running-config** command to display information about that interface. Once either a relay is found or an address allocation is found, the search stops. For example, given the following configuration:

```

interface ethernet1
 ip address 21.0.0.1 255.0.0.0
 ip address 22.0.0.5 255.0.0.0 secondary

ip dhcp pool x
 relay source 21.0.0.0 255.0.0.0
 relay destination 10.0.0.1

ip dhcp pool y
 relay source 22.0.0.0 255.0.0.0
 relay destination 20.0.0.1

```

In the following example, the DHCP client packet would be relayed to 10.0.0.1, if the SG specified ISP1 as the class name, and would be relayed to 20.0.0.1, if the SG specified ISP2 as the class name.

```

interface ethernet1
 ip address 21.0.0.1 255.0.0.0
 ip address 22.0.0.5 255.0.0.0 secondary

ip dhcp pool x
 relay source 21.0.0.0 255.0.0.0
 relay source 22.0.0.0 255.0.0.0
 case ISP1
 relay target 10.0.0.1
 case ISP2
 relay target 20.0.0.1

```

Related Commands	Command	Description
	relay source	Configures an IP address for a relay source from 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 source

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

relay source *ip-address subnet-mask*

no relay source *ip-address subnet-mask*

Syntax Description

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

Defaults

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

Command Modes

DHCP-pool configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

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 DHCP server, use the **relay target** command in DHCP pool-class configuration mode. To disable the IP address, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No target IP address is configured.

Command Modes

DHCP pool-class configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

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
```

■ relay target

```
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 forwarded by a DHCP server.

■ relay-information hex

```
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 *type number*

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

Command Modes	Mode
	User EXEC Privileged EXEC

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

Usage Guidelines The **release dhcp** command immediately releases the DHCP lease on the interface specified by the *type* and *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.

```
Router# release dhcp ethernet 3/1
```

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

Command	Description
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.

remark

To write a helpful comment (remark) for an entry in a named IP access list, use the **remark** command in access list configuration command. To remove the remark, use the **no** form of this command.

remark *remark*

no remark *remark*

Syntax Description	<i>remark</i>	Comment that describes the access-list entry, up to 100 characters long.
--------------------	---------------	--

Defaults The access-list entries have no remarks.

Command Modes Standard named or extended named access list configuration

Command History	Release	Modification
	12.0(2)T	This command was introduced.

Usage Guidelines The remark can be up to 100 characters long; anything longer is truncated.
If you want to write a comment about an entry in a numbered IP access list, use the **access-list remark** command.

Examples In the following example, the Jones subnet is not allowed to use outbound Telnet:

```
ip access-list extended telnetting
 remark Do not allow Jones subnet to telnet out
 deny tcp host 171.69.2.88 any eq telnet
```

Related Commands	Command	Description
	access-list remark	Specifies a helpful comment (remark) for an entry in a numbered IP access list.
	deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
	ip access-list	Defines an IP access list by name.
	permit (IP)	Sets conditions under which a packet passes a named IP access list.

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

<i>peer-real-ip-address</i>	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 Routing and Forwarding (VRF). A virtual IP (VIP) address cannot be used.
<i>peer-real-ip-address2</i>	(Optional) IP address of the remote peer.

Defaults

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	<i>remote-port-number</i>	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).
--------------------	---------------------------	--

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

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 *type number*

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

Command Modes	Mode
	User EXEC Privileged EXEC

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

Usage Guidelines The **renew dhcp** command immediately renews the DHCP lease for the interface specified by the *type* and *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.

```
Router# renew dhcp Ethernet 3/1
```

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

Command	Description
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.

retry (real server)

To specify how long to wait before a new connection is attempted to a failed server, use the **retry** command in SLB real server configuration mode. To restore the default retry value, use the **no** form of this command.

retry *retry-value*

no **retry**

Syntax Description

retry-value

Time, in seconds, to wait after the detection of a server failure before a new connection to the server is attempted.

If the new connection attempt succeeds, the real server is placed in **OPERATIONAL** state. If the connection attempt fails, the timer is reset, the connection is reassigned, and the process repeats until it is successful or until the server is placed **OUTOFSERVICE** by the network administrator.

Valid values range from 1 to 3600. The default value is 60 seconds.

A value of 0 means do not attempt a new connection to the server when it fails.

Defaults

The *retry-value* default is 60 seconds.

Command Modes

SLB real server configuration

Command History

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

Examples

The following example specifies that 120 seconds must elapse after the detection of a server failure before a new connection is attempted:

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 retry 120
```

Related Commands

Command	Description
real	Identifies a real server.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.