

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.

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.

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 IOS SLB NAT is configured.

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	<p>The following example specifies the client's NetBIOS type as hybrid:</p> <pre>netbios node-type h-node</pre>	
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
```

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), use the **origin** command in DHCP pool configuration mode. To disable the ODAP, use the **no** form of this command.

origin { **dhcp** | **aaa** | **ipcp** } [**subnet size initial** *size* [**autogrow** *size*]]

no origin { **dhcp** | **aaa** | **ipcp** } [**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.
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).
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).

Defaults

The default *size* value is /0.

The valid range for the *size* value is /0, and /4 to /30.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

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.

In the Cisco IOS 12.2(8)T release, the **origin** command supports only VRF-associated pools. Work is in progress to support both VRF and non-VRF pools.

Examples

The following example configures 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
```

Related Commands

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

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*
[**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*
[**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**] [**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, causing 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>	(Optional) 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 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. It 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. Some protocols allow further qualifiers described later.
<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 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.
precedence <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the section “Usage Guidelines.”
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 name as listed in the section “Usage Guidelines” of the access-list (IP extended) command.

log	<p>(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.)</p> <p>The 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.</p> <p>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.</p> <p>The logging facility may 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 due to 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.</p> <p>If you enable 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.</p>
time-range <i>time-range-name</i>	<p>(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.</p>
fragments	<p>(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.</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(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.</p>
<i>icmp-message</i>	<p>(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section “Usage Guidelines” of the access-list (IP extended) command.</p>
<i>igmp-type</i>	<p>(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 section “Usage Guidelines” of the access-list (IP extended) command.</p>

<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands 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>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, it must match the destination port.</p> <p>The range operator requires two port numbers. 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 section “Usage Guidelines” of the access-list (IP extended) command.</p> <p>TCP port names can only be used when filtering TCP. UDP port names can only be used 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 bits set. The nonmatching case is that of the initial TCP datagram to form a connection.</p>

Defaults

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 12.2(15)T.



Usage Guidelines

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

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

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack 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 data-bbox="789 296 1474 331">For an access-list entry containing only Layer 3 information:</p> <ul data-bbox="789 338 1474 405" style="list-style-type: none"> <li data-bbox="789 338 1474 405">• The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. <p data-bbox="789 422 1474 489">For an access list entry containing Layer 3 and Layer 4 information:</p> <ul data-bbox="789 495 1474 1041" style="list-style-type: none"> <li data-bbox="789 495 1474 716">• The entry is applied to nonfragmented packets and initial fragments. <ul data-bbox="854 573 1474 716" style="list-style-type: none"> <li data-bbox="854 573 1474 640">– If the entry is a permit statement, the packet or fragment is permitted. <li data-bbox="854 653 1474 716">– If the entry is a deny statement, the packet or fragment is denied. <li data-bbox="789 730 1474 1041">• 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 data-bbox="854 898 1474 1041" style="list-style-type: none"> <li data-bbox="854 898 1474 966">– If the entry is a permit statement, the noninitial fragment is permitted. <li data-bbox="854 978 1474 1041">– If the entry is a deny statement, the next access-list entry is processed. <p data-bbox="789 1056 1474 1209"> 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,	<p data-bbox="789 1215 1474 1251">The access-list entry is applied only to noninitial fragments.</p> <p data-bbox="789 1266 1474 1409"> Note The fragments keyword cannot be configured for an access-list entry that contains any Layer 4 information.</p>

Be aware that you should not simply 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 where 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 involving 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 had 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 was not policy routed or the reverse.

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 policy routing will occur as intended.

Examples

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

```
ip access-list standard Internetfilter
 deny 192.5.34.0 0.0.0.255
 permit 128.88.0.0 0.0.255.255
 permit 36.0.0.0 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 shows how to add an entry to an existing access list:

```
Router# show access-list

Standard IP access list 1
 2 permit 10.4.0.0, 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 5.5.5.5 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-list

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-list 101

Extended IP access list 101
 10 permit ip host 3.3.3.3 host 45.5.5.34
 20 permit icmp any any
 30 permit ip host 65.34.2.2 host 43.2.54.2
 40 permit ip host 45.3.4.31 host 34.3.32.3 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-list 101

Extended IP access list 101
 10 permit ip host 3.3.3.3 host 45.5.5.34
 20 permit icmp any any
 30 permit ip host 65.34.2.2 host 43.2.54.2
 40 permit ip host 45.3.4.31 host 34.3.32.3 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-list 101

Extended IP access list 101
 10 permit ip host 3.3.3.3 host 45.5.5.34
 20 permit icmp any any
 30 permit ip host 65.34.2.2 host 43.2.54.2
 40 permit ip host 45.3.4.31 host 34.3.32.3 log

Router(config)# ip access-list extended 101
Router(config-ext-nacl)# 20 permit udp host 1.1.1.1 host 2.2.2.2

Duplicate sequence number.

Router(config-ext-nacl)# end

Router# show access-list 101

Extended IP access list 101
 10 permit ip host 3.3.3.3 host 45.5.5.34
 20 permit icmp any any
 30 permit ip host 65.34.2.2 host 43.2.54.2
 40 permit ip host 45.3.4.31 host 34.3.32.3 log
```

Related Commands

Command	Description
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	Defines an IP access list by name.
ip access-list log-update	Sets the threshold number of packets that cause a logging message.

Command	Description
ip access-list resequence	Applies sequence numbers to the access list entries in an access list.
match ip-address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list.
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.

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.

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.

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

<i>retry-value</i>	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.