

## ddns (DDNS-update-method)

To specify an update method for address (A) Resource Records (RRs) as IETF standardized Dynamic Domain Name System (DDNS), use the **ddns** command in DDNS-update-method configuration mode. To disable the DDNS method for updating, use the **no** form of this command.

**ddns [both]**

**no ddns**

### Syntax Description

**both** (Optional) Both A and PTR RRs are updated.

### Defaults

No DDNS updating is configured.

### Command Modes

DDNS-update-method configuration

### Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

### Usage Guidelines

If Dynamic Host Configuration Protocol (DHCP) is used to configure the IP address on the interface, a DHCP client may not perform both A and PTR RRs or any updates. Also, if the DHCP server notifies the client during the DHCP interaction that it will perform the updates, then the DHCP client will not perform the updates. The DHCP server can always override the client even if the client is configured to perform the updates.

If the interface is configured using DHCP and if the DDNS update method is configured on that interface, then the DHCP fully qualified domain name (FQDN) option is included in the DHCP packets between the client and the server. The FQDN option contains the hostname, which is used in the update as well as information about what types of updates the client has been configured to perform.

If the **ddns** keyword is specified, the A RRs only are updated, but if the **ddns both** keyword are specified, both the A and the PTR RRs are updated. Also, if the DHCP server returns the the FQDN option with an updated hostname, that hostname is used in the update instead.

### Examples

The following example shows how to configure a DHCP server to perform both A and PTR RR updates:

```
ip ddns update method unit-test
  ddns both
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug dhcp</b>	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
<b>debug ip ddns update</b>	Enables debugging for DDNS updates.
<b>debug ip dhcp server</b>	Enables DHCP server debugging.
<b>default</b>	Specifies the command default.
<b>host (host-list)</b>	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
<b>http</b>	Specifies HTTP as the update method for A and PTR RRs.
<b>internal</b>	Specifies the internal Cisco IOS cache is used for DDNS updates of A and PTR RRs.
<b>interval maximum</b>	Specifies a maximum interval for DDNS updates of A and PTR RRs.
<b>ip ddns update hostname</b>	Enables a host to be used for DDNS updates of A and PTR RRs.
<b>ip ddns update method</b>	Enables DDNS as the update method and assigns a method name.
<b>ip dhcp client update dns</b>	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
<b>ip dhcp-client update dns</b>	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
<b>ip dhcp update dns</b>	Enables DDNS updates of A and PTR RRs for most address pools.
<b>ip host-list</b>	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
<b>show ip ddns update</b>	Displays information about the DDNS updates.
<b>show ip ddns update method</b>	Displays information about the DDNS update method.
<b>show ip dhcp server pool</b>	Displays DHCP server pool statistics.
<b>show ip host-list</b>	Displays the assigned hosts in a list.
<b>update dns</b>	Dynamically updates a DNS with A and PTR RRs for some address pools.

# default (tracking)

To set the default values for a tracked list, use the **default** command in tracking configuration mode. To disable the defaults, use the **no** form of this command.

**default** { **delay** | **object** *object-number* | **threshold percentage** }

**no default** { **delay** | **object** *object-number* | **threshold percentage** }

Syntax Description		
<b>delay</b>		Default delay value.
<b>object</b>		Default object for the list. The <i>object-number</i> argument has a valid range is from 1 to 500.
<b>threshold percentage</b>		Default threshold percentage.

**Defaults** No default behavior or values

**Command Modes** Tracking configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

**Examples** The following example shows how to configure a default threshold percentage:

```
track 3 list
 default threshold percentage
```

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

# default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** command in DHCP pool configuration mode. To remove the default router list, use the **no** form of this command.

```
default-router address [address2...address8]
```

```
no default-router
```

Syntax Description		
<i>address</i>		Specifies the IP address of a router. 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** No default behavior or values.

**Command Modes** DHCP pool configuration

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

**Usage Guidelines** The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

**Examples** The following example specifies 10.12.1.99 as the IP address of the default router:

```
default-router 10.12.1.99
```

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

# delay (tracking)

To specify a period of time to delay communicating state changes of a tracked object, use the **delay** command in tracking configuration mode. To disable the delay period, use the **no** form of this command.

**delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }

**no delay** { **up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds* }

## Syntax Description

<b>up</b>	Time to delay the notification of an up event.
<b>down</b>	Time to delay the notification of a down event.
<i>seconds</i>	Delay value, in seconds. Range is from 0 to 180. Default is 0.

## Defaults

No delay time is configured for tracking.

## Command Modes

Tracking configuration

## Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

## Usage Guidelines

This command is available to all tracked objects.

If you specify, for example, **delay up 10 down 30**, then if the object state changes from down to up, clients tracking that object are notified after 10 seconds. If the object state changes from up to down, then clients tracking that object are notified after 30 seconds.

## Examples

In the following example, the tracking process is tracking the IP-route threshold metric. The delay period to communicate the changes of the tracked object to the client process is set to 30 seconds.

```
track 1 ip route 10.22.0.0/16 metric threshold
  threshold metric up 16 down 20
  delay down 30
```

## delay (virtual server)

To change the amount of time IOS Server Load Balancing (IOS SLB) maintains TCP connection context after a connection has terminated, use the **delay** command in SLB virtual server configuration mode. To restore the default delay timer, use the **no** form of this command.

```
delay {duration | radius framed-ip duration}
```

```
no delay {duration | radius framed-ip duration}
```

### Syntax Description

<i>duration</i>	Delay timer duration for TCP connection context, in seconds. The valid range is 1 to 600 seconds. The default value is 10 seconds.
<b>radius framed-ip</b> <i>duration</i>	Delay timer for RADIUS framed-ip sticky database, in seconds. The valid range is 1 to 600 seconds. The default value is 10 seconds.

### Defaults

The default duration for the TCP connection context is 10 seconds.  
The default duration for the RADIUS framed-ip sticky database is 10 seconds.

### Command Modes

SLB virtual 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.
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 <b>radius</b> and <b>framed-ip</b> keywords and the <i>duration</i> argument were 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.

### Usage Guidelines

The TCP connection context delay timer allows out-of-sequence packets and final acknowledgments (ACKs) to be delivered after a TCP connection ends. Do not set this value to zero (0).

If you are configuring a TCP connection context delay timer for HTTP flows, choose a low number such as 5 seconds as a starting point.

For the Home Agent Director, the **delay** command has no meaning and is not supported.

### Examples

The following example specifies that IOS SLB maintains TCP connection context for 30 seconds after a connection has terminated:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# delay 30
```

■ delay (virtual server)

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip slb vservers</b>	Displays information about the virtual servers defined to IOS SLB.
<b>virtual</b>	Configures the virtual server attributes.

# deny (IP)

To set conditions in a named IP access list that will deny packets, use the **deny** command in access list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

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

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

```
no deny protocol source source-wildcard destination destination-wildcard
```

## Internet Control Message Protocol (ICMP)

```
[sequence-number] deny 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] deny 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] deny tcp source source-wildcard [operator port [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] deny udp source source-wildcard [operator port [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 deny 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"> <li>• Use a 32-bit quantity in four-part dotted-decimal format.</li> <li>• Use the <b>any</b> keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul>	
<i>source-wildcard</i>	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore.</li> <li>• Use the <b>any</b> keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul>	
<i>protocol</i>	Name or number of an Internet protocol. The <i>protocol</i> argument can be one of the keywords <b>eigrp</b> , <b>gre</b> , <b>icmp</b> , <b>igmp</b> , <b>ip</b> , <b>ipinip</b> , <b>nos</b> , <b>ospf</b> , <b>tcp</b> , or <b>udp</b> , 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 <b>ip</b> keyword. <p><b>Note</b> When the <b>icmp</b>, <b>igmp</b>, <b>tcp</b>, and <b>udp</b> 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 <b>deny</b> command.</p>	
<b>icmp</b>	Denies only ICMP packets. When you enter the <b>icmp</b> keyword, you must use the specific command syntax shown for the ICMP form of the <b>deny</b> command.	
<b>igmp</b>	Denies only IGMP packets. When you enter the <b>igmp</b> keyword, you must use the specific command syntax shown for the IGMP form of the <b>deny</b> command.	
<b>tcp</b>	Denies only TCP packets. When you enter the <b>tcp</b> keyword, you must use the specific command syntax shown for the TCP form of the <b>deny</b> command.	
<b>udp</b>	Denies only UDP packets. When you enter the <b>udp</b> keyword, you must use the specific command syntax shown for the UDP form of the <b>deny</b> 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"> <li>• Use a 32-bit quantity in four-part dotted-decimal format.</li> <li>• Use the <b>any</b> keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host destination</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li> </ul>	

<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore.</li> <li>• Use the <b>any</b> keyword as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host</b> <i>destination</i> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li> </ul>
<b>option</b> <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 <a href="#">Table 1</a> in the “Usage Guidelines” section.
<b>precedence</b> <i>precedence</i>	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.
<b>tos</b> <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 <b>access-list</b> (IP extended) command.
<b>log</b>	(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 <b>logging console</b> command.)
<b>time-range</b> <i>time-range-name</i>	(Optional) Name of the time range that applies to this <b>deny</b> statement. The name of the time range and its restrictions are specified by the <b>time-range</b> and <b>absolute</b> or <b>periodic</b> commands, respectively.
<b>fragments</b>	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the <b>fragments</b> keyword, see the “ <a href="#">Access List Processing of Fragments</a> ” and “ <a href="#">Fragments and Policy Routing</a> ” 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 <b>access-list</b> (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 <b>access-list</b> (IP extended) command.

<i>operator</i>	<p>(Optional) Compares source or destination ports. Operators include <b>lt</b> (less than), <b>gt</b> (greater than), <b>eq</b> (equal), <b>neq</b> (not equal), and <b>range</b> (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 <b>range</b> operator requires two port numbers. Up to ten port numbers can be entered for the <b>eq</b> (equal) and <b>neq</b> (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 <b>access-list</b> (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>
<b>established</b>	<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><b>Note</b> The <b>established</b> keyword can be used only with the old command-line interface (CLI) format. To use the new CLI format, you must use the <b>match-any</b> or <b>match-all</b> keywords followed by the + or - keywords and <i>flag-name</i> argument.</p>
{ <b>match-any</b>   <b>match-all</b> }	<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 <b>match-any</b> keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the <b>match-all</b> keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the <b>match-any</b> and <b>match-all</b> 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 allows IP packets if their TCP headers contain the TCP flags that are specified by the <i>flag-name</i> argument. The - keyword filters out 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: <b>urg</b>, <b>ack</b>, <b>psh</b>, <b>rst</b>, <b>syn</b>, and <b>fin</b>.</p>

**Defaults**

There are no specific conditions under which a packet is denied passing the named access list.

**Command Modes**

Access list configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(1)T	The <b>time-range</b> <i>time-range-name</i> keyword and argument were added.
	12.0(11)	The <b>fragments</b> keyword was added.
	12.2(13)T	The <b>igrp</b> 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 <b>option</b> <i>option-name</i> keyword and argument were added. The <b>match-any</b> , <b>match-all</b> , <b>+</b> , and <b>-</b> 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 <b>eq</b> and <b>neq</b> 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 specify conditions under which a packet cannot pass 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 **deny** 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 its URL: [www.iana.org](http://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 1](#).

**Table 1** 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 No Operation Option (1).
nsapa	Match packets with 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 <b>fragments</b> 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"> <li>• The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments.</li> </ul> <p>For an access list entry that contains Layer 3 and Layer 4 information:</p> <ul style="list-style-type: none"> <li>• The entry is applied to nonfragmented packets and initial fragments. <ul style="list-style-type: none"> <li>– If the entry is a <b>permit</b> statement, then the packet or fragment is permitted.</li> <li>– If the entry is a <b>deny</b> statement, then the packet or fragment is denied.</li> </ul> </li> <li>• 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"> <li>– If the entry is a <b>permit</b> statement, then the noninitial fragment is permitted.</li> <li>– If the entry is a <b>deny</b> statement, then the next access list entry is processed.</li> </ul> </li> </ul> <p><b>Note</b> The <b>deny</b> statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.</p>
...the <b>fragments</b> keyword, and assuming all of the access-list entry information matches,	The access list entry is applied only to noninitial fragments. The <b>fragments</b> 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:

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

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
Router(config)# time-range no-http
Router(config-time-range)# periodic weekdays 8:00 to 18:00
!
Router(config)# ip access-list extended strict
Router(config-ext-nacl)# deny tcp any any eq http time-range no-http
!
Router(config)# interface ethernet 0
Router(config-if)# ip access-group strict in
```

The following example adds an entry with the sequence number 25 to extended IP access list 150:

```
Router(config)# ip access-list extended 150
Router(config-std-nacl)# 25 deny ip host 172.16.3.3 host 192.168.5.34
```

The following example removes the entry with the sequence number 25 from the extended access list example shown above:

```
Router(config-std-nacl)# no 25
```

The following example sets a deny condition for an extended access list named filter2. The access list entry specifies that a packet cannot pass the named access list if it contains the Strict Source Routing Option, which is represented by the IP option value ssr.

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

The following example sets a deny condition for an extended access list named `kmdfilter1`. The access list entry specifies that a packet cannot pass the named access list if the RST and FIN TCP flags have been set for that packet:

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

The following example shows several **deny** 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 `abc`.

```
Router# show access-lists abc

Extended IP access list abc
 10 deny tcp any eq telnet any eq 450
 20 deny tcp any eq telnet any eq 679
 30 deny tcp any eq ftp any eq 450
 40 deny tcp any eq ftp any eq 679
```

Because the entries are all for the same **deny** 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 abc
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)# deny tcp any eq telnet ftp any eq 450 679
Router(config-ext-nacl)# end
```

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

```
Router# show access-lists abc

Extended IP access list abc
 10 deny tcp any eq telnet ftp any eq 450 679
```

## Related Commands

Command	Description
<b>absolute</b>	Specifies an absolute time when a time range is in effect.
<b>access-list (IP extended)</b>	Defines an extended IP access list.
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>ip access-group</b>	Controls access to an interface.
<b>ip access-list</b>	Defines an IP access list by name.
<b>ip access-list log-update</b>	Sets the threshold number of packets that cause a logging message.
<b>ip access-list resequence</b>	Applies sequence numbers to the access list entries in an access list.
<b>ip options</b>	Drops or ignores IP Options packets that are sent to the router.
<b>logging console</b>	Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
<b>match ip address</b>	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.

<b>Command</b>	<b>Description</b>
<b>periodic</b>	Specifies a recurring (weekly) time range for functions that support the time-range feature.
<b>permit (IP)</b>	Sets conditions under which a packet passes a named IP access list.
<b>remark</b>	Writes a helpful comment (remark) for an entry in a named IP access list.
<b>show access-lists</b>	Displays a group of access-list entries.
<b>show ip access-list</b>	Displays the contents of all current IP access lists.
<b>time-range</b>	Specifies when an access list or other feature is in effect.

# dns-server

To specify the Domain Name System (DNS) IP servers available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** command in DHCP pool configuration mode. To remove the DNS server list, use the **no** form of this command.

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

**no dns-server**

## Syntax Description

<i>address</i>	The IP address of a DNS 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 DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

## Command Modes

DHCP pool configuration

## Command History

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

## Usage Guidelines

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 domain name server of the client:

```
dns-server 10.12.1.99
```

## Related Commands

Command	Description
<b>domain-name (DHCP)</b>	Specifies the domain name for a DHCP client.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

## domain-name (DHCP)

To specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** command in DHCP pool configuration mode. To remove the domain name, use the **no** form of this command.

**domain-name** *domain*

**no domain-name**

### Syntax Description

<i>domain</i>	Specifies the domain name string of the client.
---------------	---

### Defaults

No default behavior or values.

### Command Modes

DHCP pool configuration

### Command History

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

### Examples

The following example specifies cisco.com as the domain name of the client:

```
domain-name cisco.com
```

### Related Commands

Command	Description
<b>dns-server</b>	Specifies the DNS IP servers available to a DHCP client.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

# dynamic

To define a named dynamic IP access list, use the **dynamic** command in access-list configuration mode. To remove the access lists, use the **no** form of this command.

```
dynamic dynamic-name [timeout minutes] {deny | permit} protocol source source-wildcard
destination destination-wildcard [precedence precedence] [tos tos] [log] [fragments]
```

```
no dynamic dynamic-name
```

## Internet Control Message Protocol (ICMP)

```
dynamic dynamic-name [timeout minutes] {deny | permit} icmp source source-wildcard
destination destination-wildcard [icmp-type [icmp-code] | icmp-message]
[precedence precedence] [tos tos] [log] [fragments]
```

## Internet Group Management Protocol (IGMP)

```
dynamic dynamic-name [timeout minutes] {deny | permit} igmp source source-wildcard
destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log]
[fragments]
```

## Transmission Control Protocol (TCP)

```
dynamic dynamic-name [timeout minutes] {deny | permit} tcp source source-wildcard
[operator [port]] destination destination-wildcard [operator [port]] [established] [precedence
precedence] [tos tos] [log] [fragments]
```

## User Datagram Protocol (UDP)

```
dynamic dynamic-name [timeout minutes] {deny | permit} udp source source-wildcard
[operator [port]] destination destination-wildcard [operator [port]] [precedence precedence]
[tos tos] [log] [fragments]
```

### Syntax Description

<i>dynamic-name</i>	Identifies this access list as a dynamic access list. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <i>Cisco IOS Security Configuration Guide</i> .
<b>timeout</b> <i>minutes</i>	(Optional) Specifies the absolute length of time (in minutes) that a temporary access-list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the <i>Cisco IOS Security Configuration Guide</i> .
<b>deny</b>	Denies access if the conditions are matched.
<b>permit</b>	Permits access if the conditions are matched.
<i>protocol</i>	Name or number of an Internet protocol. It can be one of the keywords <b>eigrp</b> , <b>gre</b> , <b>icmp</b> , <b>igmp</b> , <b>ip</b> , <b>ipinip</b> , <b>nos</b> , <b>ospf</b> , <b>tcp</b> , or <b>udp</b> , 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 <b>ip</b> keyword. Some protocols allow further qualifiers described later.

<i>source</i>	<p>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</p> <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted decimal format.</li> <li>• Use the <b>any</b> keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul>
<i>source-wildcard</i>	<p>Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:</p> <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore.</li> <li>• Use the <b>any</b> keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host source</b> as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.</li> </ul>
<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted decimal format.</li> <li>• Use the <b>any</b> keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host destination</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li> </ul>
<i>destination-wildcard</i>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <ul style="list-style-type: none"> <li>• Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore.</li> <li>• Use the <b>any</b> keyword as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.</li> <li>• Use <b>host destination</b> as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.</li> </ul>
<b>precedence</b> <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.”
<b>tos</b> <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.”

<b>log</b>	<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 <b>logging console</b> 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>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 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>
<b>fragments</b>	<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 <b>fragments</b> 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.”</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.”</p>
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include <b>lt</b> (less than), <b>gt</b> (greater than), <b>eq</b> (equal), <b>neq</b> (not equal), and <b>range</b> (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 <b>range</b> 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 <b>access-list</b> (IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.</p>
<b>established</b>	<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**

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

**Command Modes**

Access-list configuration

**Command History**

Release	Modification
11.2	This command was introduced.
12.0(11)	The <b>fragments</b> keyword was added.
12.2(13)T	The <b>igrp</b> keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.

**Usage Guidelines**

You can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the ToS value, or the precedence of the packet.

**Caution**

Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

**Note**

After an access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**
- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type names and ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**
- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**

- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**
- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**



- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a **?** in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xmcp**

#### **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 <b>fragments</b> keyword (the default behavior), and assuming all of the access-list entry information matches,	<p>For an access-list entry containing only Layer 3 information:</p> <ul style="list-style-type: none"> <li>• The entry is applied to nonfragmented packets, initial fragments and noninitial fragments.</li> </ul> <p>For an access-list entry containing Layer 3 and Layer 4 information:</p> <ul style="list-style-type: none"> <li>• The entry is applied to nonfragmented packets and initial fragments. <ul style="list-style-type: none"> <li>– If the entry is a <b>permit</b> statement, the packet or fragment is permitted.</li> <li>– If the entry is a <b>deny</b> statement, the packet or fragment is denied.</li> </ul> </li> <li>• 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"> <li>– If the entry is a <b>permit</b> statement, the noninitial fragment is permitted.</li> <li>– If the entry is a <b>deny</b> statement, the next access-list entry is processed.</li> </ul> </li> </ul> <p> <b>Note</b> The <b>deny</b> statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.</p>
...the <b>fragments</b> keyword, and assuming all of the access-list entry information matches,	<p> <b>Note</b> The access-list entry is applied only to noninitial fragments. The <b>fragments</b> 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 defines a dynamic access list named washington:

```
ip access-group washington in
!
ip access-list extended washington
dynamic testlist timeout 5
permit ip any any
permit tcp any host 185.302.21.2 eq 23
```

**Related Commands**

Command	Description
<b>clear access-template</b>	Clears a temporary access-list entry from a dynamic access list manually.
<b>distribute-list in (IP)</b>	Filters networks received in updates.
<b>distribute-list out (IP)</b>	Suppresses networks from being advertised in updates.
<b>ip access-group</b>	Controls access to an interface.
<b>ip access-list</b>	Defines an IP access list by name.
<b>logging console</b>	Limits messages logged to the console based on severity.
<b>show access-lists</b>	Displays the contents of current IP and rate-limit access lists.
<b>show ip access-list</b>	Displays the contents of all current IP access lists.

# faildetect

To specify the conditions that indicate a server failure, use the **faildetect** SLB real server configuration command. To restore the default values that indicate a server failure, use the **no** form of this command.

**faildetect numconns** *number-conns* [**numclients** *number-clients*]

**no faildetect**

## Syntax Description

<b>numconns</b>	Number of consecutive TCP connection reassignments allowed before a real server is considered to have failed.
<i>number-conns</i>	Connection reassignment threshold value in the range from 1 to 255. The default is 8 connection failures.
<b>numclients</b>	(Optional) Number of unique client connection failures allowed before a real server is considered to have failed.
<i>number-clients</i>	(Optional) Client connection reassignment threshold value in the range from 1 to 8. The default is 2 client connection failures.

## Defaults

If you do not specify the **faildetect** command, the default value of the connection reassignment threshold is 8.

If you do not specify the **numclients** keyword, the default value of the unique client failure threshold is 2.

## 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

In the following example the connection reassignment threshold is set to 16 and, because the **numclients** keyword is not configured, the threshold for unique client connection failure is set to the default value 8. The real server is considered to have failed when 8 unique clients have had connection failures and there have been 16 connection reassignments.

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 faildetect numconns 16
```

## Related Commands

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

# forwarding-agent

To specify the port on which the forwarding agent will listen for wildcard and fixed affinities, use the **forwarding-agent** CASA-port configuration command. To disable listening on that port, use the **no** form of the command.

**forwarding-agent** *port-number* [*password* [*timeout*]]

**no forwarding-agent**

## Syntax Description

<i>port-number</i>	Port numbers on which the forwarding agent will listen for wildcards broadcast from the services manager. This must match the port number defined on the services manager.
<i>password</i>	(Optional) Text password used for generating the MD5 digest.
<i>timeout</i>	(Optional) Duration (in seconds) during which the Forwarding Agent will accept the new and old password. Valid range is from 0 to 3600 seconds. The default is 180 seconds.

## Defaults

The default password timeout is 180 seconds.  
The default port for the services manager is 1637.

## Command Modes

CASA-port configuration

## Command History

Release	Modification
12.0(5)T	This command was introduced.

## Examples

The following example specifies that the forwarding agent will listen for wildcard and fixed affinities on port 1637:

```
forwarding-agent 1637
```

## Related Commands

Command	Description
<b>show ip casa oper</b>	Displays operational information about the Forwarding Agent.

# glbp authentication

To configure an authentication string for the Gateway Load Balancing Protocol (GLBP), use the **glbp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

```
glbp group-number authentication {text string | md5 {key-string [0 | 7] key | key-chain name-of-chain}}
```

```
no glbp group-number authentication {text string | md5 {key-string [0 | 7] key | key-chain name-of-chain}}
```

## Syntax Description

<i>group-number</i>	GLBP group number in the range from 0 to 1023.
<b>text</b> <i>string</i>	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
<b>md5</b>	Message Digest 5 (MD5) authentication.
<b>key-string</b> <i>key</i>	Specifies the secret key for MD5 authentication. The number of characters in the command plus the key string must not exceed 255 characters. We recommend using at least 16 characters.
<b>0</b>	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
<b>7</b>	(Optional) Encrypted key.
<b>key-chain</b> <i>name-of-chain</i>	Identifies a group of authentication keys.

## Defaults

No authentication of GLBP messages occurs.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(2)T	The <b>md5</b> keyword and associated parameters were added.

## Usage Guidelines

The same authentication method must be configured on all the routers that are configured to be members of the same GLBP group, to ensure interoperability. A router will ignore all GLBP messages that contain the wrong authentication information.

If password encryption is configured with the **service password-encryption** command, the software saves the key string in the configuration as encrypted text.

## Examples

The following example configures stringxyz as the authentication string required to allow GLBP routers in group 10 to interoperate:

```
interface fastethernet 0/0
  glbp 10 authentication text stringxyz
```

In the following example, GLBP queries the key chain “AuthenticateGLBP” to obtain the current live key and key ID for the specified key chain:

```
key chain AuthenticateGLBP
  key 1
    key-string ThisIsASecretKey

interface Ethernet0/1
  ip address 10.0.0.1 255.255.255.0
  glbp 2 ip 10.0.0.10
  glbp 2 authentication md5 key-chain AuthenticateGLBP
```

**Related Commands**

Command	Description
<b>glbp ip</b>	Enables GLBP.
<b>service password-encryption</b>	Encrypts passwords.

# glbp forwarder preempt

To configure a router to take over as active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **glbp forwarder preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]

**no glbp** *group* **forwarder preempt** [**delay minimum**]

Syntax Description		
	<i>group</i>	GLBP group number in the range from 0 to 1023.
	<b>delay minimum</b> <i>seconds</i>	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

**Command Default** Forwarder preemption is enabled with a default delay of 30 seconds.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(14)S	This command was introduced.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Examples** The following example shows a router being configured to preempt the current AVF when the current AVF falls below its low weighting threshold. If the router preempts the current AVF, it waits 60 seconds before taking over the role of the AVF.

```
glbp 10 forwarder preempt delay minimum 60
```

Related Commands	Command	Description
	<b>glbp ip</b>	Enables GLBP.

# glbp ip

To activate the Gateway Load Balancing Protocol (GLBP), use the **glbp ip** command in interface configuration mode. To disable GLBP, use the **no** form of this command.

```
glbp group ip [ip-address [secondary]]
```

```
no glbp group ip [ip-address [secondary]]
```

## Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
<i>ip-address</i>	(Optional) Virtual IP address for the GLBP group. The IP address must be in the same subnet as the interface IP address.
<b>secondary</b>	(Optional) Indicates that the IP address is a secondary GLBP virtual address.

## Defaults

GLBP is disabled by default.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Usage Guidelines

The **glbp ip** command activates GLBP on the configured interface. If an IP address is specified, that address is used as the designated virtual IP address for the GLBP group. If no IP address is specified, the designated address is learned from another router configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one router on the cable must have been configured with the designated address. A router must be configured with, or have learned, the virtual IP address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ip** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

## Examples

The following example activates GLBP for group 10 on Fast Ethernet interface 0/0. The virtual IP address to be used by the GLBP group is set to 10.21.8.10.

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 ip 10.21.8.10
```

The following example activates GLBP for group 10 on Fast Ethernet interface 0/0. The virtual IP address used by the GLBP group will be learned from another router configured to be in the same GLBP group.

```
interface fastethernet 0/0
 glbp 10 ip
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show glbp</b>	Displays GLBP information.

---

# glbp load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **glbp load-balancing** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]

**no glbp** *group* **load-balancing**

## Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
<b>host-dependent</b>	(Optional) Specifies a load balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
<b>round-robin</b>	(Optional) Specifies a load balancing method where each virtual forwarder in turn is included in address resolution replies for the virtual IP address. This method is the default.
<b>weighted</b>	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

## Defaults

The round-robin method is the default.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Usage Guidelines

Use the host-dependent method of GLBP load balancing when you need each host to always use the same router. Use the weighted method of GLBP load balancing when you need unequal load balancing because routers in the GLBP group have different forwarding capacities.

## Examples

The following example shows the host-dependent load-balancing method being configured for the AVG of the GLBP group 10:

```
interface fastethernet 0/0
 glbp 10 ip 10.21.8.10
 glbp 10 load-balancing host-dependent
```

## Related Commands

Command	Description
<b>show glbp</b>	Displays GLBP information.

# glbp name

To enable IP redundancy by assigning a name to the Gateway Load Balancing Protocol (GLBP) group, use the **glbp name** command in interface configuration mode. To disable IP redundancy for a group, use the **no** form of this command.

**glbp** *group-number* **name** *group-name*

**no glbp** *group-number* **name** *group-name*

## Syntax Description

<i>group-number</i>	GLBP group number. Range is from 0 to 1023.
<i>group-name</i>	GLBP group name specified as a character string. Maximum number of characters is 255.

## Defaults

IP redundancy for a group is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.3(7)T	This command was introduced.

## Usage Guidelines

The GLBP redundancy client must be configured with the same GLBP group name so that the redundancy client and the GLBP group can be connected.

## Examples

The following example assigns the abccomp name to GLBP group 10:

```
glbp 10 name abccomp
```

## Related Commands

Command	Description
<b>glbp authentication</b>	Configures an authentication string for the GLBP.
<b>glbp forwarder preempt</b>	Configures a router to take over as AVF for a GLBP group if it has higher priority than the current AVF.
<b>glbp ip</b>	Activates GLBP.
<b>glbp load-balancing</b>	Specifies the load-balancing method used by the AVG of GLBP.
<b>glbp preempt</b>	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
<b>glbp priority</b>	Sets the priority level of the gateway within a GLBP group.
<b>glbp timers</b>	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.

<b>Command</b>	<b>Description</b>
<b>glbp timers redirect</b>	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
<b>glbp weighting</b>	Specifies the initial weighting value of the GLBP gateway.
<b>glbp weighting track</b>	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
<b>show glbp</b>	Displays GLBP information.
<b>track</b>	Configures an interface to be tracked where the GLBP weighting changes based on the state of the interface.

# glbp preempt

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has higher priority than the current AVG, use the **glbp preempt** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**glbp group preempt** [**delay minimum** *seconds*]

**no glbp group preempt** [**delay minimum**]

## Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
<b>delay minimum</b> <i>seconds</i>	(Optional) Specifies a minimum number of seconds that the router will delay before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

## Defaults

A GLBP router with a higher priority than the current AVG cannot assume the role of AVG. The default delay value is 30 seconds.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Examples

The following example shows a router being configured to preempt the current AVG when its priority of 254 is higher than that of the current AVG. If the router preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
glbp 10 preempt delay minimum 60
glbp 10 priority 254
```

## Related Commands

Command	Description
<b>glbp ip</b>	Enables GLBP.
<b>glbp priority</b>	Sets the priority level of the router within a GLBP group.

# glbp priority

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **glbp priority** command in interface configuration mode. To remove the priority level of the gateway, use the **no** form of this command.

**glbp** *group* **priority** *level*

**no glbp** *group* **priority** *level*

Syntax Description	group	GLBP group number in the range from 0 to 1023.
	level	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

**Defaults** *level*: 100

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(14)S	This command was introduced.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

**Usage Guidelines** Use this command to control which virtual gateway becomes the active virtual gateway (AVG). After the priorities of several different virtual gateways are compared, the gateway with the numerically higher priority is elected as the AVG. If two virtual gateways have equal priority, the gateway with the higher IP address is selected.

**Examples** The following example shows a virtual gateway being configured with a priority of 254:

```
glbp 10 priority 254
```

Related Commands	Command	Description
	<b>glbp ip</b>	Enables GLBP.
	<b>glbp preempt</b>	Configures a router to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

# glbp timers redirect

To configure the time during which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF), use the **glbp timers redirect** command in interface configuration mode. To restore the redirect timers to their default values, use the **no** form of this command.

**glbp group timers redirect** *redirect timeout*

**no glbp group timers redirect** *redirect timeout*

Syntax Description	group	GLBP group number in the range from 0 to 1023.
	<i>redirect</i>	Redirect timer interval (in seconds). The default is 300 seconds (5 minutes).
	<i>timeout</i>	Time (in seconds) before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Defaults	<i>redirect</i> : 300 seconds <i>timeout</i> : 14,400 seconds
----------	--

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.2(14)S	This command was introduced.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines	<p>A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. If the virtual forwarder has learned the virtual MAC address from hello messages, it is referred to as a secondary virtual forwarder.</p> <p>The redirect timer sets the time delay between a forwarder failing on the network and the AVG assuming that the forwarder will not return. The virtual MAC address to which the forwarder was responsible for replying to is still given out in Address Resolution Protocol (ARP) replies, but the forwarding task is handled by another router in the GLBP group.</p> <p>The timeout interval is the time delay between a forwarder failing on the network and the MAC address for which the forwarder was responsible becoming inactive on all of the routers in the GLBP group. After the timeout interval, packets sent to this virtual MAC address will be lost. The timeout interval must be long enough to allow all hosts to refresh their ARP cache entry that contained the virtual MAC address.</p>
------------------	---

**Examples**

The following example shows GLBP group 1, on Fast Ethernet interface 0/0, being configured with a redirect timer of 600 seconds (10 minutes), and a timeout interval of 7200 seconds (2 hours):

```
interface fastethernet 0/0
  glbp 10 ip
  glbp 10 timers redirect 600 7200
```

# glbp timers

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

```
glbp group timers [msec] hellotime [msec] holdtime
```

```
no glbp group timers
```

## Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
<b>msec</b>	(Optional) Specifies that the following ( <i>hellotime</i> or <i>holdtime</i> ) argument value will be expressed in milliseconds.
<i>hellotime</i>	Hello interval. The default is 3 seconds (3000 milliseconds).
<i>holdtime</i>	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The default is 10 seconds (10,000 milliseconds).

## Defaults

*hellotime*: 3 seconds  
*holdtime*: 10 seconds

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Usage Guidelines

Routers on which timer values are not configured can learn timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All routers in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Normally, holdtime is greater than three times the value of hello time, ( $holdtime > 3 * hellotime$ ). The range of values for holdtime force the holdtime to be greater than the hello time.

## Examples

The following example shows the GLBP group 10 on Fast Ethernet interface 0/0 timers being configured for an interval of 5 seconds between hello packets, and the time after which virtual gateway and virtual forwarder information is considered to be invalid to 18 seconds:

```
interface fastethernet 0/0
 glbp 10 ip
 glbp 10 timers 5 18
```

# glbp weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **glbp weighting track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

```
glbp group weighting track object-number [decrement value]
```

```
no glbp group weighting track object-number [decrement value]
```

## Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
<i>object-number</i>	Object number representing an item to be tracked. Use the <b>track</b> command to configure the tracked object.
<b>decrement</b> <i>value</i>	(Optional) Specifies an amount by which the GLBP weighting for the router is decremented (or incremented) when the interface goes down (or comes back up). The value range is from 1 to 254, with a default value of 10.

## Defaults

The default decrement value is 10.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Usage Guidelines

This command ties the weighting of the GLBP gateway to the availability of its interfaces. It is useful for tracking interfaces that are not configured for GLBP.

When a tracked interface goes down, the GLBP gateway weighting decreases by 10. If an interface is not tracked, its state changes do not affect the GLBP gateway weighting. For each GLBP group, you can configure a separate list of interfaces to be tracked.

The optional *value* argument specifies by how much to decrement the GLBP gateway weighting when a tracked interface goes down. When the tracked interface comes back up, the weighting is incremented by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface to be tracked.

## Examples

In the following example, Fast Ethernet interface 0/0 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

```
interface fastethernet 0/0
```

■ **glbp weighting track**

```
ip address 10.21.8.32 255.255.255.0
glbp 10 weighting track 1
glbp 10 weighting track 2 decrement 5
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>glbp weighting</b>	Specifies the initial weighting value of a GLBP gateway.
<b>track</b>	Configures an interface to be tracked.

# glbp weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **glbp weighting** command in interface configuration mode. To restore the default values, use the **no** form of this command.

```
glbp group weighting maximum [lower lower] [upper upper]
```

```
no glbp group weighting
```

## Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
<i>maximum</i>	Maximum weighting value in the range from 1 to 254. Default value is 100.
<b>lower lower</b>	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
<b>upper upper</b>	(Optional) Specifies an upper weighting value in the range from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

## Defaults

The default gateway weighting value is 100 and the default lower weighting value is 1.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Usage Guidelines

The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the router fails, the weighting value of the router may fall from the maximum value to below the lower threshold, causing the router to give up its role as a virtual forwarder. When the weighting value of the router rises above the upper threshold, the router can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to configure parameters for an interface to be tracked. If an interface on a router goes down, the weighting for the router can be reduced by a specified value.

## Examples

The following example shows the weighting of the gateway for GLBP group 10 being set to a maximum of 110 with a lower weighting limit of 95 and an upper weighting limit of 105:

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 weighting 110 lower 95 upper 105
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>glbp weighting track</b>	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
<b>track</b>	Configures an interface to be tracked.

# hardware-address

To specify the hardware address of a Dynamic Host Configuration Protocol (DHCP) client, use the **hardware-address** DHCP pool configuration command. It is valid for manual bindings only. To remove the hardware address, use the **no** form of this command.

**hardware-address** *hardware-address type*

**no hardware-address**

## Syntax Description

<i>hardware-address</i>	Specifies the MAC address of the hardware platform of the client.
<i>type</i>	Indicates the protocol of the hardware platform. Strings and values are acceptable. The string options are: <ul style="list-style-type: none"> <li>• ethernet</li> <li>• ieee802</li> </ul> The value options are: <ul style="list-style-type: none"> <li>• 1 10Mb Ethernet</li> <li>• 6 IEEE 802</li> </ul> If no type is specified, the default protocol is Ethernet.

## Defaults

Ethernet is the default type if none is specified.

## Command Modes

DHCP pool configuration

## Command History

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

## Examples

The following example specifies b708.1388.f166 as the MAC address of the client:

```
hardware-address b708.1388.f166 ieee802
```

## Related Commands

Command	Description
<b>client-identifier</b>	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
<b>host</b>	Specifies the IP address and network mask for a manual binding to a DHCP client.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

## host (host-list)

To specify a list of hosts that will receive Dynamic Domain Name System (DDNS) updates of address (A) and pointer (PTR) Resource Records (RRs), use the **host** command in host-list configuration mode. To disable the host list, use the **no** form of this command.

**host** {*host-ip-address* | *hostname*} [**vrf** *vrf-name*]

**no host** {*host-ip-address* | *hostname*} [**vrf** *vrf-name*]

### Syntax Description

<i>host-ip-address</i>	List of server IP addresses that will receive DDNS updates.
<i>hostname</i>	Specifies a hostname.
<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies the Virtual Private Network (VPN) and routing and forwarding table. The <i>vrf-name</i> argument is a name with which the address pool is associated.

### Defaults

No list is configured for hosts.

### Command Modes

Host-list configuration

### Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

### Examples

The following example shows how to configure a list of hosts:

```
ip host-list test
 host 10.10.0.0 vrf RED
```

### Related Commands

Command	Description
<b>debug dhcp</b>	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
<b>debug ip ddns update</b>	Enables debugging for DDNS updates.
<b>debug ip dhcp server</b>	Enables DHCP server debugging.
<b>ip ddns update hostname</b>	Enables a host to be used for DDNS updates of A and PTR RRs.
<b>ip ddns update method</b>	Specifies a method of DDNS updates of A and PTR RRs and the maximum interval between the updates.
<b>ip dhcp client update dns</b>	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.

<b>Command</b>	<b>Description</b>
<b>ip dhcp-client update dns</b>	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
<b>ip dhcp update dns</b>	Enables DDNS updates of A and PTR RRs for most address pools.
<b>ip host-list</b>	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
<b>show ip ddns update</b>	Displays information about the DDNS updates.
<b>show ip ddns update method</b>	Displays information about the DDNS update method.
<b>show ip dhcp server pool</b>	Displays DHCP server pool statistics.
<b>show ip host-list</b>	Displays the assigned hosts in a list.
<b>update dns</b>	Dynamically updates a DNS with A and PTR RRs for some address pools.

# host

To specify the IP address and network mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client, use the **host** command in DHCP pool configuration mode. To remove the IP address of the client, use the **no** form of this command.

```
host address [mask | prefix-length]
```

```
no host
```

## Syntax Description

<i>address</i>	Specifies the IP address of the client.
<i>mask</i>	(Optional) Specifies the network mask of the client.
<i>prefix-length</i>	(Optional) Specifies 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 (/).

## Command Modes

DHCP pool configuration

## Command History

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

## Usage Guidelines

If the mask and prefix length are unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used. This command is valid for manual bindings only.

There is no limit on the number of manual bindings but you can configure only one manual binding per host pool.

## Examples

The following example specifies 10.12.1.99 as the IP address of the client and 255.255.248.0 as the subnet mask:

```
host 10.12.1.99 255.255.248.0
```

## Related Commands

Command	Description
<b>client-identifier</b>	Specifies the unique identifier of a Microsoft DHCP client in dotted hexadecimal notation.
<b>hardware-address</b>	Specifies the hardware address of a DHCP client.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
<b>network (DHCP)</b>	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

## http (DDNS-update-method)

To specify an update method for address (A) and pointer (PTR) Resource Records (RRs) as HTTP and enter DDNS-HTTP configuration mode, use the **http** command in DDNS-update-method configuration mode. To disable HTTP dynamic updates, use the **no** form of this command.

```
http {add url-string | remove url-string}
```

```
no http
```

Syntax Description	
<b>add</b> <i>url-string</i>	<p>URL to be used to add or change a mapping between a hostname and an IP address. The <i>url-string</i> argument takes the following form:</p> <pre>http://userid:password@domain-name/update-folder-name/update?system=<i>system-name</i>&amp;hostname=<i>hostname</i>&amp;myip=<i>myipaddr</i></pre> <ul style="list-style-type: none"> <li>• <i>userid</i> and <i>password</i>—Strings for the organization website that you use for performing the A and PTR RRs updates.</li> <li>• <i>domain-name</i>—String for the organizational URL that you are using for the updates; for example www.Cisco.com.</li> <li>• <i>update-folder-name</i>—String of the folder name within the organizational website in which your updates are stored.</li> <li>• <b>update?system=<i>system-name</i></b>—Update system (method) being used; for example, dydns is DDNS and dyn is EasyDNS.</li> </ul> <p><b>Note</b> Before entering the question mark (?) character, press the control (Ctrl) key and the v key together on your keyboard. This will allow you to enter the ? without the software interpreting the ? as a help query.</p> <ul style="list-style-type: none"> <li>• <b>&amp;hostname=<i>hostname</i></b>—Hostname to update.</li> <li>• <b>&amp;myip=<i>myipaddr</i></b>—IP address with which the specified hostname is associated, respectively.</li> </ul> <p><b>Note</b> There is one additional special character string, &lt;s&gt;, which could also be entered into the <i>url-string</i>. If &lt;s&gt; is entered, when the update is processed, the IP address of the server to which the update is being sent is substituted at that location.</p>
<b>remove</b> <i>url-string</i>	<p>URL to be used to remove a mapping between a hostname and an IP address. The <i>url-string</i> argument takes the same form as the one shown in the <b>add</b> keyword description.</p>

**Defaults** No HTTP update method is configured.

**Command Modes** DDNS-update-method configuration

**Command History**

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

**Examples**

The following example shows how to specify the DynDNS.org to process the updates:

```
ip ddns update method unit-test
  http add http://myuserid:secret@members.dyndns.org/nic/update?system=dyndns&hostname=
mywebsite&myip=10.10.10.10
```

The following are examples of URLs that can be used to update some HTTP DNS update services. These URLs are correct to the best of the knowledge of Cisco but have not been tested in all cases. Where the word “USERNAME:” appears in the URL, your account username at the HTTP site should be used. Where the word “PASSWORD” appears in the URL, your password for that account should be used:

**DDNS**

```
http://USERNAME:PASSWORD@members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
```

!Requires “interval max 28 0 0 0” in the update method definition.

**TZO**

```
http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>&Email=USERNAME&TZOKey=PASSWORD&IP
Address=<a>
```

**EASYDNS**

```
http://USERNAME:PASSWORD@members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&
host_id=<h>
```

**JUSTLINUX**

```
http://USERNAME:PASSWORD@www.justlinux.com/bin/controlpanel/dyndns/jlc.pl?direst=1&
username=USERNAME&password=PASSWORD&host=<h>&ip=<a>
```

**DYNS**

```
http://USERNAME:PASSWORD@www.dyns.cx/postscript.php?username=USERNAME&password=PASSWORD&
host=<h>&ip=<a>
```

**HN**

```
http://USERNAME:PASSWORD@dup.hn.org/vanity/update?ver=1&IP=<a>
```

**ZONEEDIT**

```
http://USERNAME:PASSWORD@www.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
```

**Note**

Because these services are provided by the respective companies, the URLs may be subject to change or the service could be discontinued at any time. Cisco takes no responsibility for the accuracy or use of any of this information. The URLs were obtained using an application called “ez-ipupdate,” which is available for free on the Internet.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ddns</b>	Specifies DDNS as the update method for A and PTR RRs.
<b>debug dhcp</b>	Displays debugging information about the DHCP client and monitors the status of DHCP packets.
<b>debug ip ddns update</b>	Enables debugging for DDNS updates.
<b>debug ip dhcp server</b>	Enables DHCP server debugging.
<b>default</b>	Specifies the command default.
<b>host (host-list)</b>	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
<b>internal</b>	Specifies the internal Cisco IOS cache is used for DDNS updates of A and PTR RRs.
<b>interval maximum</b>	Specifies a maximum interval for DDNS updates of A and PTR RRs.
<b>ip ddns update hostname</b>	Enables a host to be used for DDNS updates of A and PTR RRs.
<b>ip ddns update method</b>	Enables DDNS as the update method and assigns a method name.
<b>ip dhcp client update dns</b>	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
<b>ip dhcp-client update dns</b>	Enables DDNS updates of A RRs using the same hostname passed in the hostname and FQDN options by a client.
<b>ip dhcp update dns</b>	Enables DDNS updates of A and PTR RRs for most address pools.
<b>ip host-list</b>	Specifies a list of hosts that will receive DDNS updates of A and PTR RRs.
<b>show ip ddns update</b>	Displays information about the DDNS updates.
<b>show ip ddns update method</b>	Displays information about the DDNS update method.
<b>show ip dhcp server pool</b>	Displays DHCP server pool statistics.
<b>show ip host-list</b>	Displays the assigned hosts in a list.
<b>update dns</b>	Dynamically updates a DNS with A and PTR RRs for some address pools.