



## Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services

Release 12.3 T

Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Text Part Number: OL-4707-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*  
Copyright © 2003-2004 Cisco Systems, Inc. All rights reserved.



**Introduction** IP1R-1

**IP Addressing and Services Commands** IP1R-11





# Introduction

---

This book describes the commands used to configure and monitor the following IP addressing and services capabilities and features:

- IP Addressing
- Dynamic Host Configuration Protocol (DHCP)
- IP Services
- IP Access Lists
- Server Load Balancing
- Web Cache Communications Protocol (WCCP)

For IP addressing and services tasks and examples, refer to the “IP Addressing and Services” part in the *Cisco IOS IP Configuration Guide*, Release 12.3.

## IP Addressing

Use the following commands to configure and monitor IP addressing:

- arp authorized
- arp (global)
- arp (interface)
- arp timeout
- clear arp-cache
- clear arp interface
- clear host
- clear ip nat translation
- clear ip nhrp
- clear ip route
- clear ip snat sessions
- clear ip snat translation distributed
- clear ip snat translation peer
- crypto ipsec

- ip address
- ip broadcast-address
- ip cef traffic-statistics
- ip classless
- ip default-gateway
- ip directed-broadcast
- ip dns spoofing
- ip domain list
- ip domain lookup
- ip domain name
- ip domain retry
- ip domain timeout
- ip domain round-robin
- ip forward-protocol
- ip forward-protocol spanning-tree
- ip forward-protocol turbo-flood
- ip helper address
- ip host
- ip irdp
- ip name-server
- ip nat
- ip nat inside destination
- ip nat inside source
- ip nat outside source
- ip nat pool
- ip nat service
- ip nat stateful id
- ip nat translation max-entries
- ip nat translation (timeout)
- ip netmask-format
- ip nhrp authentication
- ip nhrp holdtime
- ip nhrp interest
- ip nhrp map
- ip nhrp map multicast
- ip nhrp map multicast dynamic
- ip nhrp max-send
- ip nhrp network-id

- ip nhrp nhs
- ip nhrp record
- ip nhrp responder
- ip nhrp server-only
- ip nhrp trigger-svc
- ip nhrp use
- ip proxy-arp
- ip routing
- ip routing
- ip subnet zero
- ip unnumbered
- no ip gratuitous-arps
- show arp
- show hosts
- show ip aliases
- show ip arp
- show ip interface
- show ip irdp
- show ip masks
- show ip nat statistics
- show ip nat translations
- show ip nhrp
- show ip nhrp traffic
- show ip snat
- term ip netmask-format

## DHCP

Use the following commands to configure and monitor DHCP:

- address range
- accounting (DHCP)
- bootfile
- class
- clear ip dhcp binding
- clear ip dhcp server statistics
- clear ip dhcp subnet
- clear ip route dhcp
- client-identifier

- client-name
- default-router
- dns-server
- domain-name (DHCP)
- hardware-address
- host
- import all
- ip address dhcp
- ip address pool (DHCP)
- ip dhcp aaa default username
- ip dhcp bootp ignore
- ip dhcp class
- ip dhcp-client broadcast-flag
- ip dhcp-client default-router distance
- ip dhcp client class-id
- ip dhcp client client-id
- ip dhcp client hostname
- ip dhcp client lease
- ip dhcp client request
- ip dhcp conflict logging
- ip dhcp database
- ip dhcp excluded-address
- ip dhcp limit lease per interface
- ip dhcp limited-broadcast-address
- ip dhcp ping packets
- ip dhcp ping timeout
- ip dhcp pool
- ip dhcp relay forward spanning-tree
- ip dhcp relay information check
- ip dhcp relay information option
- ip dhcp relay information policy
- ip dhcp relay information trusted
- ip dhcp relay information trust-all
- ip dhcp smart-relay
- lease
- netbios-name-server
- netbios-node-type
- network (DHCP)



- next-server
- option
- origin
- relay agent information
- relay-information hex
- release dhcp
- renew dhcp
- service dhcp
- show ip dhcp binding
- show ip dhcp conflict
- show ip dhcp database
- show ip dhcp import
- show ip dhcp pool
- show ip dhcp server statistics
- show ip route dhcp
- subnet prefix-length
- update arp
- utilization mark high
- utilization mark low
- vrf

## IP Access Lists

Use the following commands to configure and monitor access lists:

- access-class
- access-list (IP extended)
- access-list (IP standard)
- access-list compiled
- access-list remark
- clear access-list counters
- deny (IP)
- dynamic
- ip access-group
- ip access-list resequence
- ip access-list
- ip options
- permit
- remark

- show access-lists
- show access-list compiled
- show ip access-list

## IP Services

Use the following commands to configure and monitor IP services:

- clear ip accounting
- clear ip drp
- clear tcp statistics
- clear time-range ipc
- delay (tracking)
- dynamic
- forwarding-agent
- glbp authentication
- glbp forwarder preempt
- glbp ip
- glbp load-balancing
- glbp name
- glbp preempt
- glbp priority
- glbp timers
- glbp timers redirect
- glbp weighting track
- ip access-group
- ip accounting
- ip accounting-list
- ip accounting-threshold
- ip accounting-transits
- ip accounting mac-address
- ip accounting precedence
- ip casa
- ip drp access-group
- ip drp authentication key-chain
- ip drp server
- ip icmp rate-limit unreachable
- ip icmp redirect
- ip information-reply

- ip mask-reply
- ip vrf
- ip mtu
- ip redirects
- ip source-route
- ip tcp chunk-size
- ip tcp compression-connections
- ip tcp ecn
- ip tcp header-compression
- ip tcp path-mtu-discovery
- ip tcp queuemax
- ip tcp selective-ack
- ip tcp synwait-time
- ip tcp timestamp
- ip tcp window-size
- ip unreachable
- object (tracking)
- threshold metric
- threshold percentage
- threshold weight
- track list
- track resolution
- show access-list compiled
- show glbp
- show interface mac
- show interface precedence
- show ip access-list
- show ip accounting
- show ip casa affinities
- show ip casa oper
- show ip casa stats
- show ip casa wildcard
- show ip drp
- show ip redirects
- show ip sockets
- show ip tcp header-compression
- show ip traffic
- show standby

- show standby delay
- show tcp statistics
- show time-range ipc
- show track
- show vrrp
- show vrrp interface
- standby authentication
- standby delay minimum reload
- standby ip
- standby mac-address
- standby mac-refresh
- standby name
- standby preempt
- standby priority
- standby redirects
- standby timers
- standby track
- standby use-bia
- standby version
- start-forwarding-agent
- threshold metric
- threshold percentage
- threshold weight
- track interface
- track ip route
- track list
- track resolution
- track rtr
- track timer
- transmit-interface
- vrrp authentication
- vrrp description
- vrrp ip
- vrrp preempt
- vrrp priority
- vrrp timers advertise
- vrrp timers learn
- vrrp track

# Server Load Balancing

Use the following commands to configure and monitor server load balancing:

- advertise
- agent
- bindid
- clear ip slb
- client
- delay (virtual server)
- faildetect
- idle
- inservice (DFP agent)
- inservice (real server)
- inservice (virtual server)
- interval (DFP agent)
- ip dfp agent
- ip slb dfp
- ip slb serverfarm
- ip slb vserver
- maxconns
- nat
- password (DFP agent)
- port (DFP agent)
- predictor
- real
- reassign
- retry (real server)
- serverfarm
- show ip dfp
- show ip slb dfp
- show ip slb reals
- show ip slb serverfarms
- show ip slb stats
- show ip slb sticky
- show ip slb vservers

- sticky
- synguard
- virtual
- weight

## WCCP

Use the following commands to configure and monitor WCCP:

- clear ip wccp
- ip wccp
- ip wccp enable
- ip wccp group-listen
- ip wccp redirect exclude in
- ip wccp redirect exclude in
- ip wccp redirect-list
- ip wccp redirect
- ip wccp version
- ip web-cache redirect'
- show ip wccp
- show ip wccp web-caches



## IP Addressing and Services Commands

---

# access-class

To restrict incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list, use the **access-class** command in line configuration mode. To remove access restrictions, use the **no** form of this command.

```
access-class access-list-number { in [vrf-also] | out }
```

```
no access-class access-list-number { in | out }
```

## Syntax Description

<i>access-list-number</i>	Number of an IP access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
<b>in</b>	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
<b>vrf-also</b>	Accepts incoming connections from interfaces that belong to a VRF.
<b>out</b>	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

## Defaults

No access lists are defined.

## Command Modes

Line configuration

## Command History

Release	Modification
10.0	This command was introduced.
12.2	The <b>vrf-also</b> keyword was added.

## Usage Guidelines

Remember to set *identical restrictions* on all the virtual terminal lines because a user can connect to any of them.

To display the access lists for a particular terminal line, use the **show line EXEC** command and specify the line number.

If you do not specify the **vrf-also** keyword, incoming Telnet connections from interfaces that are part of a VRF are rejected.

## Examples

The following example defines an access list that permits only hosts on network 192.89.55.0 to connect to the virtual terminal ports on the router:

```
access-list 12 permit 192.89.55.0 0.0.0.255
 line 1 5
 access-class 12 in
```

The following example defines an access list that denies connections to networks other than network 36.0.0.0 on terminal lines 1 through 5:



```
access-list 10 permit 36.0.0.0 0.255.255.255
line 1 5
access-class 10 out
```

**Related Commands**

Command	Description
<b>show line</b>	Displays the parameters of a terminal line.

## access-list (IP extended)

To define an extended IP access list, use the extended version of the **access-list** command in global configuration mode. To remove the access lists, use the **no** form of this command.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
  protocol source source-wildcard destination destination-wildcard [precedence precedence]
  [tos tos] [log | log-input] [time-range time-range-name] [fragments]
```

```
no access-list access-list-number
```

### Internet Control Message Protocol (ICMP)

```
access-list access-list-number [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 | log-input] [time-range
  time-range-name] [fragments]
```

### Internet Group Management Protocol (IGMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
  igmp source source-wildcard destination destination-wildcard [igmp-type]
  [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]
  [fragments]
```

### Transmission Control Protocol (TCP)

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

### User Datagram Protocol (UDP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit}
  udp source source-wildcard [operator [port]] destination destination-wildcard
  [operator [port]] [precedence precedence] [tos tos] [log | log-input] [time-range
  time-range-name] [fragments]
```

#### Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 100 to 199 or from 2000 to 2699.
<b>dynamic</b> <i>dynamic-name</i>	(Optional) 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>pim</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 below.
<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 source. Each wildcard bit 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet will be considered a match to this access list entry. <p>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> <p>Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.</p>
<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>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination 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 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 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 may drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.</p>
<b>log-input</b>	(Optional) Includes the input interface and source MAC address or VC in the logging output.
<b>time-range</b> <i>time-range-name</i>	(Optional) Name of the time range that applies to this statement. The name of the time range and its restrictions are specified by the <b>time-range</b> command.
<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 ICMP message type and code name. The possible names are listed in the section “Usage Guidelines.”
<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 section “Usage Guidelines.”
<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>	(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.” TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.  TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
<b>established</b>	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, SYN, or URG control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
<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.

**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**

Global configuration

**Command History**

Release	Modification
10.0	This command was introduced.
10.3	The following keywords and arguments were added: <ul style="list-style-type: none"> <li>• <i>source</i></li> <li>• <i>source-wildcard</i></li> <li>• <i>destination</i></li> <li>• <i>destination-wildcard</i></li> <li>• <b>precedence</b> <i>precedence</i></li> <li>• <i>icmp-type</i></li> <li>• <i>icmp-code</i></li> <li>• <i>icmp-message</i></li> <li>• <i>igmp-type</i></li> <li>• <i>operator</i></li> <li>• <i>port</i></li> <li>• <b>established</b></li> </ul>
11.1	The <b>dynamic</b> <i>dynamic-name</i> keyword and argument were added.
11.1	The <b>timeout</b> <i>minutes</i> keyword and argument were added.
11.2	The <b>log-input</b> keyword was added.

Release	Modification
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>non500-isakmp</b> keyword was added to the list of UDP port names. The <b>igrp</b> keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.

## Usage Guidelines

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the 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 type of service (ToS) value, or the precedence of the packet.



### Note

After a numbered 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 numbered 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**
- **dnsix**
- **domain**
- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **non500-isakmp**
- **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..
<p>...no <b>fragments</b> keyword (the default behavior), and assuming all of the access-list entry information matches,</p>	<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>
<p>...the <b>fragments</b> keyword, and assuming all of the access-list entry information matches,</p>	<p>The access-list entry is applied only to noninitial fragments.</p> <p> <b>Note</b> 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**

In the following example, serial interface 0 is part of a Class B network with the address 128.88.0.0, and the address of the mail host is 128.88.1.2. The **established** keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicates that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
interface serial 0
 ip access-group 102 in
```

The following example permits Domain Naming System (DNS) packets and ICMP echo and echo reply packets:

```
access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp any host 128.88.1.2 eq smtp
access-list 102 permit tcp any any eq domain
access-list 102 permit udp any any eq domain
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
```

The following examples show how wildcard bits are used to indicate the bits of the prefix or mask that are relevant. Wildcard bits are similar to the bitmasks that are used with normal access lists. Prefix or mask bits corresponding to wildcard bits set to 1 are ignored during comparisons and prefix or mask bits corresponding to wildcard bits set to 0 are used in comparison.

The following example permits 192.108.0.0 255.255.0.0 but denies any more specific routes of 192.108.0.0 (including 192.108.0.0 255.255.255.0):

```
access-list 101 permit ip 192.108.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example permits 131.108.0/24 but denies 131.108/16 and all other subnets of 131.108.0.0:

```
access-list 101 permit ip 131.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 131.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

The following example uses a time range to deny HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
 !
access-list 101 deny tcp any any eq http time-range no-http
 !
interface ethernet 0
 ip access-group 101 in
```

## Related Commands

Command	Description
<b>access-class</b>	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>access-list remark</b>	Writes a helpful comment (remark) for an entry in a numbered IP access list.
<b>clear access-template</b>	Clears a temporary access list entry from a dynamic access list.
<b>delay (tracking)</b>	Sets conditions under which a packet does not pass a named access list.
<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>ip accounting</b>	Enables IP accounting on an interface.
<b>logging console</b>	Controls which messages are logged to the console, 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.
<b>permit (IP)</b>	Sets conditions under which a packet passes a named 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 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.
<b>time-range</b>	Specifies when an access list or other feature is in effect.

## access-list (IP standard)

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

```
access-list access-list-number { deny | permit } source [source-wildcard] [log]
```

```
no access-list access-list-number
```

<b>Syntax Description</b>	<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 99 or from 1300 to 1999.
	<b>deny</b>	Denies access if the conditions are matched.
	<b>permit</b>	Permits access if the conditions are matched.
	<i>source</i>	Number of the network or host from which the packet is being sent. There are two 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> </ul>
	<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the source. There are two 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 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> </ul>
	<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.)  The message includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. 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.  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.

**Defaults** The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

**Command Modes** Global configuration

**Command History**

Release	Modification
10.3	This command was introduced.
11.3(3)T	The <b>log</b> keyword was added.

**Usage Guidelines**

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control vty access, and restrict the contents of routing updates.

Use the **show access-lists EXEC** command to display the contents of all access lists.

Use the **show ip access-list EXEC** command to display the contents of one access list.

**Caution**

Enhancements to this command are backward compatible; migrating from releases prior to Cisco IOS Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This condition could cause you severe security problems.** Save your old configuration file before booting these images.

**Examples**

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.5.34.0 0.0.0.255
access-list 1 permit 128.88.0.0 0.0.255.255
access-list 1 permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

The following example of a standard access list allows access for devices with IP addresses in the range from 10.29.2.64 to 10.29.2.127. All packets with a source address not in this range will be rejected.

```
access-list 1 permit 10.29.2.64 0.0.0.63
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3 0.0.0.0
```

**Related Commands**

Command	Description
<b>access-class</b>	Restricts incoming and outgoing connections between a particular vty (into a Cisco device) and the addresses in an access list.
<b>access-list (IP extended)</b>	Defines an extended IP access list.
<b>access-list remark</b>	Writes a helpful comment (remark) for an entry in a numbered IP access list.
<b>deny (IP)</b>	Sets conditions under which a packet does not pass a named access list.
<b>distribute-list in (IP)</b>	Filters networks received in updates.

Command	Description
<b>distribute-list out (IP)</b>	Suppresses networks from being advertised in updates.
<b>ip access-group</b>	Controls access to an interface.
<b>permit (IP)</b>	Sets conditions under which a packet passes a named access list.
<b>remark (IP)</b>	Writes a helpful comment (remark) for an entry in a named IP access list.
<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.

# access-list compiled

To enable the Turbo Access Control Lists (Turbo ACL) feature, use the **access-list compiled** command in global configuration mode. To disable the Turbo ACL feature, use the **no** form of this command.

**access-list compiled**

**no access-list compiled**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** Global configuration

## Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

## Usage Guidelines

By default, the Turbo ACL feature is disabled. When Turbo ACL is disabled, normal ACL processing is enabled, and no ACL acceleration occurs.

When the Turbo ACL feature is enabled using the **access-list compiled** command, the ACLs in the configuration are scanned and, if suitable, compiled for Turbo ACL acceleration. This scanning and compilation may take a few seconds when the system is processing large and complex ACLs, or when the system is processing a configuration that contains a large number of ACLs.

Any configuration change to an ACL that is being accelerated, such as the addition of new ACL entries or the deletion of the ACL, triggers a recompilation of that ACL.

When Turbo ACL tables are being built (or rebuilt) for a particular ACL, the normal sequential ACL search is used until the new tables are ready for installation.

## Examples

The following example enables the Turbo ACL feature:

```
access-list compiled
```



# access-list remark

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

**access-list** *access-list-number* **remark** *remark*

**no access-list** *access-list-number* **remark** *remark*

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

**Defaults** The access list entries have no remarks.

**Command Modes** Global configuration

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

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

**Examples** In the following example, the workstation belonging to Jones is allowed access, and the workstation belonging to Smith is not allowed access:

```
access-list 1 remark Permit only Jones workstation through
access-list 1 permit 171.69.2.88
access-list 1 remark Do not allow Smith workstation through
access-list 1 deny 171.69.3.13
```

Related Commands	Command	Description
	<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-list</b>	Defines an IP access list by name.
	<b>remark</b>	Writes a helpful comment (remark) for an entry in a named IP access list.

# accounting (DHCP)

To enable DHCP accounting, use the **accounting** command in DHCP pool configuration mode. To disable DHCP accounting for the specified server group, use the **no** form of this command.

**accounting** *server-group-name*

**no accounting** *server-group-name*

<b>Syntax Description</b>	<i>server-group-name</i>	Name of a server group to apply DHCP accounting. The server group can have one or more members. The server group is defined in the configuration of the <b>aaa group server</b> and <b>aaa accounting</b> commands.
---------------------------	--------------------------	---

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(15)T	This command was introduced.

**Usage Guidelines**

The **accounting** DHCP pool configuration command is used to enable the DHCP accounting feature by sending secure DHCP START accounting messages when IP addresses are assigned to DHCP clients, and secure DHCP STOP accounting messages when DHCP leases are terminated. A DHCP lease is terminated when the client explicitly releases the lease, when the session times out, and when the DHCP bindings are cleared from the DHCP database. DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

The **accounting** command can be used only to network pools in which bindings are created automatically and destroyed upon lease termination (or when the client sends a DHCP RELEASE message). DHCP bindings are also destroyed when the **clear ip dhcp binding** or **no service dhcp** command is issued. These commands should be used with caution if an address pool is configured with DHCP accounting.

AAA and RADIUS must be configured before this command can be used to enable DHCP accounting. A server group must be defined with the **aaa group server** command. START and STOP message generation is configured with the **aaa accounting** command. The **aaa accounting** command can be configured to enable the DHCP accounting to send both START and STOP messages or STOP messages only.

**Examples**

The following example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group.

```
Router(config)# ip dhcp pool WIRELESS-POOL
Router(dhcp-config)# accounting RADIUS-GROUP1
Router(dhcp-config)# exit
```

**Related Commands**

Command	Description
<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
<b>aaa group server</b>	Groups different server hosts into distinct lists and distinct methods.
<b>aaa new-model</b>	Enables the AAA access control model.
<b>aaa session-id</b>	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
<b>clear arp-cache</b>	Deletes all dynamic entries from the ARP cache.
<b>clear ip dhcp binding</b>	Deletes an automatic address binding from the Cisco IOS DHCP server database.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
<b>ip radius source-interface</b>	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
<b>radius-server host</b>	Specifies a RADIUS server host.
<b>radius-server retransmit</b>	Specifies the number of times that IOS will look for RADIUS server hosts.
<b>service dhcp</b>	Enables the Cisco IOS DHCP server and relay agent features.
<b>show ip dhcp binding</b>	Displays address bindings on the Cisco IOS DHCP server.
<b>show ip dhcp server statistics</b>	Displays Cisco IOS DHCP server statistics.
<b>update arp</b>	Secures the MAC address of the authorized client interface to the DHCP binding.

# address range

To set an address range for a DHCP class in a DHCP server address pool, use the **address range** command in DHCP pool class configuration mode. To remove the address range, use the **no** form of this command.

**address range** *start-ip end-ip*

**no address range** *start-ip end-ip*

Syntax Description	<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
	<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.

**Defaults** No default behavior or values

**Command Modes** DHCP pool class configuration

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

**Usage Guidelines** If this command is not configured for a DHCP class in a DHCP server address pool, the default value is the entire subnet of the address pool.

**Examples** The following example sets the available address range for class 1 from 10.0.20.1 through 10.0.20.100:

```
ip dhcp pool ABC
network 10.0.20.0 255.255.255.0
class CLASS1
address range 10.0.20.1 10.0.20.100
```

Related Commands	Command	Description
	<b>ip dhcp class</b>	Defines a DHCP class and enters DHCP class configuration mode.

# advertise

To control the installation of a static route to the Null0 interface for a virtual server address, use the **advertise** SLB virtual server configuration command. To prevent the installation of a static route for the virtual server IP address, use the **no** form of this command.

**advertise**

**no advertise**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The SLB virtual server IP address is added to the routing table.

**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.

**Usage Guidelines** By default, virtual server addresses are *advertised*. That is, static routes to the Null0 interface are installed for the virtual server addresses.

Advertisement of this static route using the routing protocol requires that you configure redistribution of static routes for the routing protocol.

**Examples** The following example prevents advertisement of the IP address of the virtual server in routing protocol updates:

```
ip slb vserver PUBLIC_HTTP
no advertise
```

Related Commands	Command	Description
	<b>show ip slb vservers</b>	Displays information about the virtual servers.

# agent

To configure a Dynamic Feedback Protocol (DFP) agent, use the **agent** SLB command in DFP configuration mode. To remove an agent definition from the DFP configuration, use the **no** form of this command.

```
agent ip-address port [timeout [retry-count [retry-interval]]]
```

```
no agent ip-address port
```

Syntax Description	
<i>ip-address</i>	Agent IP address.
<i>port</i>	Agent port number.
<i>timeout</i>	(Optional) Time period (in seconds) during which the DFP manager must receive an update from the DFP agent. The default is 0 seconds, which means there is no timeout.
<i>retry-count</i>	(Optional) Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. The default is 0 retries, which means there are infinite retries.
<i>retry-interval</i>	(Optional) Interval (in seconds) between retries. The default is 180 seconds.

**Defaults**

The default timeout is 0 seconds (no timeout).  
 The default retry count is 0 (infinite retries).  
 The default retry interval is 180 seconds.

**Command Modes** SLB DFP 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.

**Usage Guidelines**

You can configure up to 1024 agents.

A DFP agent collects status information about the load capability of a server and reports that information to a load manager. The DFP agent may reside on the server, or it may be a separate device that collects and consolidates the information from several servers before reporting to the load manager.

**Examples**

The following example configures a DFP agent on the DFP manager, sets the DFP password to *Cookies* and the timeout to *360* seconds, changes the configuration mode to DFP configuration mode, sets the IP address of the DFP agent to *10.1.1.1*, and sets the port number of the DFP agent to *2221* (FTP):

```
ip slb dfp password Cookies 360
agent 10.1.1.1 2221
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip slb dfp</b>	Configures the IOS SLB DFP.

# arp (global)

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the **arp** command in global configuration mode. To remove an entry from the ARP cache, use the **no** form of this command.

**arp** *ip-address hardware-address type* [**alias**]

**no arp** *ip-address hardware-address type* [**alias**]

Syntax Description		
	<i>ip-address</i>	IP address in four-part dotted decimal format corresponding to the local data-link address.
	<i>hardware-address</i>	Local data-link address (a 48-bit address).
	<i>type</i>	Encapsulation description. For Ethernet interfaces, this is typically the <b>arpa</b> keyword. For FDDI and Token Ring interfaces, this is always the <b>snap</b> keyword.
	<b>alias</b>	(Optional) Indicates that the Cisco IOS software should respond to ARP requests as if it were the owner of the specified address.

**Defaults** No entries are permanently installed in the ARP cache.

**Command Modes** Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** The Cisco IOS software uses ARP cache entries to translate 32-bit IP addresses into 48-bit hardware addresses.

Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries.

To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

**Examples** The following is an example of a static ARP entry for a typical Ethernet host:

```
arp 192.31.7.19 0800.0900.1834 arpa
```

Related Commands	Command	Description
	<b>clear arp-cache</b>	Deletes all dynamic entries from the ARP cache.



# arp (interface)

To control the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, Frame Relay, and Token Ring hardware addresses, use the **arp** command in interface configuration mode. To disable an encapsulation type, use the **no** form of this command.

```
arp { arpa | frame-relay | snap }
```

```
no arp { arpa | frame-relay | snap }
```

Syntax Description	Command	Description
	<b>arpa</b>	Standard Ethernet-style Address Resolution Protocol (ARP) (RFC 826).
	<b>frame-relay</b>	Enables ARP over a Frame Relay encapsulated interface.
	<b>snap</b>	ARP packets conforming to RFC 1042.

**Defaults** Standard Ethernet-style ARP

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(13)T	The <b>probe</b> keyword was removed because the HP Probe feature is no longer available in Cisco IOS software.

**Usage Guidelines** Unlike most commands that have multiple arguments, the **arp** command has arguments that are not mutually exclusive. Each command enables or disables a specific type of ARP.

Given a network protocol address (IP address), the **arp frame-relay** command determines the corresponding hardware address, which would be a data-link connection identifier (DLCI) for Frame Relay.

The **show interfaces EXEC** command displays the type of ARP being used on a particular interface. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

**Examples** The following example enables frame relay services:

```
interface ethernet 0
  arp frame-relay
```

Related Commands	Command	Description
	<b>clear arp-cache</b>	Deletes all dynamic entries from the ARP cache.
	<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.

# arp authorized

To disable dynamic Address Resolution Protocol (ARP) learning on an interface, use the **arp authorized** command in interface configuration mode. To reenable dynamic ARP learning, use the **no** form of this command.

**arp authorized**

**no arp authorized**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Interface configuration

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

**Usage Guidelines** The **arp authorized** command disables dynamic ARP learning on an interface. This command enhances security in public wireless LANs (PWLANS) by limiting the leasing of IP addresses to mobile users to authorized users. The IP address to MAC address mapping for that interface can be installed only by the authorized subsystem. Unauthorized clients can not respond to ARP requests.

If both static and authorized ARP are installing the same ARP entry, static configuration overrides authorized ARP. You can install a static ARP entry by using the **arp** global configuration command. You can only remove a nondynamic ARP entry by the same method in which it was installed.

You can only use this command on Ethernet interfaces.

**Examples** The following example disables dynamic ARP learning on interface Ethernet 0:

```
interface Ethernet0
ip address 10.0.0.1 255.255.255.0
arp authorized
```

Related Commands	Command	Description
	<b>arp (global)</b>	Adds a permanent entry in the ARP cache.
	<b>update arp</b>	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

# arp probe interval

To control the probing of authorized peers, use the **arp probe interval** command in interface configuration mode. To disable the probe, use the **no** form of this command.

**arp probe interval** *interval-number* **count** *count-number*

**no arp probe interval** *interval-number* **count** *count-number*

<b>Syntax Description</b>	<i>interval-number</i>	Interval in seconds after which the next probe will be sent to see if the peer is still present. The range is from 1 to 10.
	<b>count</b> <i>count-number</i>	Number of probe retries. If no response, the peer has logged off. The range is from 1 to 60.

**Defaults** Disabled

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(8)XX	This command was introduced.

**Usage Guidelines** Once you configure the **arp probe interval** command, probing continues until you disable it using the **no** form of the command on all interfaces.

**Examples** The following example shows a 2-second interval with a probe of the peer occurring 5 times:

```
interface ethernet 0
  arp probe interval 2 count 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	arp (interface)	Controls the interface-specific handling of IP address resolution.
	<b>clear arp-cache</b>	Deletes all dynamic entries from the ARP cache.
	<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.

# arp timeout

To configure how long an entry remains in the Address Resolution Protocol (ARP) cache, use the **arp timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**arp timeout** *seconds*

**no arp timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Time (in seconds) that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.
---------------------------	----------------	--

<b>Defaults</b>	14400 seconds (4 hours)
-----------------	-------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Usage Guidelines** This command is ignored when issued on interfaces that do not use ARP. The **show interfaces EXEC** command displays the ARP timeout value. The value follows the “Entry Timeout:” heading, as seen in the following example from the **show interfaces** command:

```
ARP type: ARPA, PROBE, Entry Timeout: 14400 sec
```

**Examples** The following example sets the ARP timeout to 12000 seconds to allow entries to time out more quickly than the default:

```
interface ethernet 0
  arp timeout 12000
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.

# bindid

To configure a bind ID, use the **bindid** command in SLB server farm configuration mode. To remove a bind ID from the server farm configuration, use the **no** form of this command.

**bindid** [*bind-id*]

**no bindid** [*bind-id*]

<b>Syntax Description</b>	<i>bind-id</i> (Optional) Bind ID number. The default bind ID is 0.
---------------------------	---

<b>Defaults</b>	The default bind ID is 0.
-----------------	---------------------------

<b>Command Modes</b>	SLB server farm configuration
----------------------	-------------------------------

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

<b>Usage Guidelines</b>	You can configure one bind ID on each <b>bindid</b> command.
-------------------------	--

The bind ID allows a single physical server to be bound to multiple virtual servers and report a different weight for each one. Thus, the single real server is represented as multiple instances of itself, each having a different bind ID. DFP uses the bind ID to identify for which instance of the real server a given weight is specified.

<b>Examples</b>	The following example configures bind ID 309:
-----------------	---

```
ip slb serverfarm PUBLIC
bindid 309
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip slb dfp</b>	Configures the IOS SLB DFP.

# bootfile

To specify the name of the default boot image for a Dynamic Host Configuration Protocol (DHCP) client, use the **bootfile** command in DHCP pool configuration mode. To delete the boot image name, use the **no** form of this command.

**bootfile** *filename*

**no bootfile**

<b>Syntax Description</b>	<i>filename</i>	Specifies the name of the file that is used as a boot image.
---------------------------	-----------------	--

<b>Defaults</b>	No default behavior or values.	
-----------------	--------------------------------	--

<b>Command Modes</b>	DHCP pool configuration	
----------------------	-------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Examples</b>	The following example specifies xllboot as the name of the boot file:	
-----------------	---	--

```
bootfile xllboot
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
	<b>next-server</b>	Configures the next server in the boot process of a DHCP client.

## class (dhcp)

To associate a class with a DHCP address pool and enter DHCP pool class configuration mode, use the **class** command in DHCP pool configuration mode. To remove the class association, use the **no** form of this command.

**class** *class-name*

**no class** *class-name*

<b>Syntax Description</b>	<i>class-name</i>	Name of the DHCP class.
---------------------------	-------------------	-------------------------

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

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

<b>Usage Guidelines</b>	You first define the class using the <b>ip dhcp class</b> global configuration command. If a nonexistent class is named by the <b>class</b> command, the class will be automatically created. Each class in the DHCP pool will be examined for a match in the order configured.
-------------------------	---

<b>Examples</b>	The following example associates DHCP class 1 and class 2 with a DHCP pool named ABC:
-----------------	---

```
ip dhcp pool ABC
network 10.0.20.0 255.255.255.0
class CLASS1
address range 10.0.20.1 10.0.20.100
class CLASS2
address range 10.0.20.101 10.0.20.200
```

Related Commands	Command	Description
	<b>ip dhcp class</b>	Defines a DHCP class and enters DHCP class configuration mode.

# clear access-list counters

To clear the counters of an access list, use the **clear access-list counters** command in privileged EXEC mode.

**clear access-list counters** {*access-list-number* | *access-list-name*}

Syntax Description	<i>access-list-number</i>	Access list number of the access list for which to clear the counters.
	<i>access-list-name</i>	Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.0	This command was introduced.

Usage Guidelines	Some access lists keep counters that count the number of packets that pass each line of an access list. The <b>show access-lists</b> command displays the counters as a number of matches. Use the <b>clear access-list counters</b> command to restart the counters for a particular access list to 0.
------------------	---

Examples	The following example clears the counters for access list 101:
----------	--

```
Router# clear access-list counters 101
```

Related Commands	Command	Description
	<b>show access-lists</b>	Displays the contents of current IP and rate-limit access lists.



# clear arp interface

To clear the entire Address Resolution Protocol (ARP) cache on an interface, use the **clear arp interface** command in EXEC mode.

**clear arp interface** *type number*

Syntax Description	<i>type</i>	Interface type.
	<i>number</i>	Interface number.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	<b>Release</b>	<b>Modification</b>
	12.0(22)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 **clear arp interface** command to clean up ARP entries associated with an interface.

**Examples** The following example clears the ARP cache from Ethernet interface 0:

```
Router# clear arp interface ethernet 0
```

# clear arp-cache

To delete all dynamic entries from the Address Resolution Protocol (ARP) cache, to clear the fast-switching cache, and to clear the IP route cache, use the **clear arp-cache** command in EXEC mode.

**clear arp-cache**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** EXEC

---

Command History	Release	Modification
	10.0	This command was introduced.

---



---

**Examples** The following example removes all dynamic entries from the ARP cache and clears the fast-switching cache:

```
clear arp-cache
```

---

Related Commands	Command	Description
	<b>arp (global)</b>	Adds a permanent entry in the ARP cache.
	<b>arp (interface)</b>	Controls the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, and Token Ring hardware addresses.

---

# clear host

To delete entries from the host name-to-address cache, use the **clear host** EXEC command.

```
clear host {name | *}
```

Syntax Description	<i>name</i>	Particular host entry to remove.
	*	Removes all entries.

**Command Modes** EXEC

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** The host name entries will not be removed from NVRAM, but will be cleared in running memory.

**Examples** The following example clears all entries from the host name-to-address cache:

```
clear host *
```

Related Commands	Command	Description
	<b>ip host</b>	Defines a static host name-to-address mapping in the host cache.
	<b>show hosts</b>	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses.

# clear ip accounting

To clear the active or checkpointed database when IP accounting is enabled, use the **clear ip accounting** command in privileged EXEC mode.

**clear ip accounting [checkpoint]**

<b>Syntax Description</b>	<b>checkpoint</b> (Optional) Clears the checkpointed database.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	You can also clear the checkpointed database by issuing the <b>clear ip accounting</b> command twice in succession.
-------------------------	---

<b>Examples</b>	The following example clears the active database when IP accounting is enabled:
-----------------	---

```
Router> clear ip accounting
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip accounting</b>	Enables IP accounting on an interface.
	<b>ip accounting-list</b>	Defines filters to control the hosts for which IP accounting information is kept.
	<b>ip accounting-threshold</b>	Sets the maximum number of accounting entries to be created.
	<b>ip accounting-transit</b>	Controls the number of transit records that are stored in the IP accounting database.
	<b>show ip accounting</b>	Displays the active accounting or checkpointed database or displays access list violations.

# clear ip dhcp binding

To delete an automatic address binding from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp binding** command in privileged EXEC mode.

```
clear ip dhcp [pool name] binding { * | address }
```

Syntax Description	pool name	(Optional) Name of the DHCP pool.
	*	Clears all automatic bindings.
	<i>address</i>	The address of the binding you want to clear.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.2(8)T	The <b>pool name</b> keyword and argument combination was added.

**Usage Guidelines** Typically, the address denotes the IP address of the client. If the asterisk (\*) character is used as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp pool** global configuration command to delete a manual binding.

Note the following behavior for the **clear ip dhcp binding** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified binding.
- If you do not specify the **pool name** option and the \* option is specified, it is assumed that all automatic or on-demand bindings in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the \* option, all automatic or on-demand bindings in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified binding will be deleted from the specified pool.

## Examples

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
Router# clear ip dhcp binding 10.12.1.99
```

The following example deletes all bindings from all pools:

```
Router# clear ip dhcp binding *
```

The following example deletes all bindings from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 binding *
```

**clear ip dhcp binding**

The following example deletes address binding 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool red binding pool2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip dhcp binding</b>	Displays address bindings on the Cisco IOS DHCP server.

# clear ip dhcp conflict

To clear an address conflict from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp conflict** command in privileged EXEC mode.

```
clear ip dhcp [pool name] conflict { * | address }
```

Syntax Description		
	<b>pool name</b>	(Optional) Name of the DHCP pool.
	*	Clears all address conflicts.
	<i>address</i>	The IP address of the host that contains the conflicting address you want to clear.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.0(1)T	This command was introduced.
	12.2(8)T	The <b>pool name</b> keyword and argument combination were added.

**Usage Guidelines**

The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If the asterisk (\*) character is used as the address parameter, DHCP clears all conflicts.

Note the following behavior for the **clear ip dhcp conflict** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified conflict.
- If you do not specify the **pool name** option and the \* option is specified, it is assumed that all automatic/ or on-demand conflicts in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the \* option, all automatic or on-demand conflicts in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the specified conflict will be deleted from the specified pool.

**Examples**

The following example shows an address conflict of 10.12.1.99 being deleted from the DHCP server database:

```
Router# clear ip dhcp conflict 10.12.1.99
```

The following example deletes all address conflicts from all pools:

```
Router# clear ip dhcp conflict *
```

The following example deletes all address conflicts from the address pool named pool1:

```
Router# clear ip dhcp pool pool1 conflict *
```

**clear ip dhcp conflict**

The following example deletes address conflict 10.13.2.99 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 conflict 10.13.2.99
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip dhcp conflict</b>	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.



# clear ip dhcp server statistics

To reset all Cisco IOS Dynamic Host Configuration Protocol (DHCP) server counters, use the **clear ip dhcp server statistics** command in privileged EXEC mode.

**clear ip dhcp server statistics**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** The **show ip dhcp server statistics** command displays DHCP counters. All counters are cumulative. The counters will be initialized, or set to zero, with the **clear ip dhcp server statistics** command.

**Examples** The following example resets all DHCP counters to zero:

```
Router# clear ip dhcp server statistics
```

Related Commands	Command	Description
	<b>show ip dhcp server statistics</b>	Displays Cisco IOS DHCP server statistics.

# clear ip dhcp subnet

To clear all currently leased subnets in the Cisco IOS Dynamic Host Configuration Protocol (DHCP) pool, use the **clear ip dhcp subnet** command in privileged EXEC configuration mode.

```
clear ip dhcp [pool name] subnet { * | address }
```

Syntax Description	<i>pool name</i>	(Optional) Name of the DHCP pool.
	*	Clears all leased subnets.
	<i>address</i>	Clears a subnet containing the specified IP address.

**Command Modes** Privileged EXEC

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

## Usage Guidelines

A PPP session that is allocated an IP address from the released subnet will be reset.

Note the following behavior for the **clear ip dhcp subnet** command:

- If you do not specify the **pool name** option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified subnet.
- If you do not specify the **pool name** option and the \* option is specified, it is assumed that all automatic or on-demand subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool name** option and the \* option, all automatic or on-demand subnets in the specified pool only will be cleared.
- If you specify the **pool name** option and an IP address, the subnet containing the specified IP address will be deleted from the specified pool.



### Caution

Use this command with caution to prevent undesired termination of active PPP sessions.

## Examples

The following example releases the subnet containing 10.0.0.2 from any non-VRF on-demand address pools:

```
Router# clear ip dhcp subnet 10.0.0.2
```

The following example clears all leased subnets from all pools:

```
Router# clear ip dhcp subnet *
```

The following example clears all leased subnets from the address pool named pool3:

```
Router# clear ip dhcp pool pool3 subnet *
```

The following example clears the address 10.0.0.2 from the address pool named pool2:

```
Router# clear ip dhcp pool pool2 subnet 10.0.0.2
```

---

**Related Commands**

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

# clear ip drp

To clear all statistics being collected on Director Response Protocol (DRP) requests and replies, use the **clear ip drp** command in privileged EXEC mode.

## clear ip drp

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

**Examples** The following example clears all DRP statistics:

```
Router> clear ip drp
```

Related Commands	Command	Description
	<b>ip drp access-group</b>	Controls the sources of DRP queries to the DRP Server Agent.
	<b>ip drp authentication key-chain</b>	Configures authentication on the DRP Server Agent for DistributedDirector.

# clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in EXEC mode.

```
clear ip nat translation [* | [inside global-ip global-port local-ip local-port] / [outside local-ip global-ip] [esp | tcp | udp]]
```

```
clear ip nat translation [* | [inside global-ip global-port local-ip local-port] / [outside local-ip global-ip] [esp | tcp | udp]]
```

Syntax Description		
<b>*</b>		Clears all dynamic translations.
<b>inside</b>		(Optional) Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
<i>global-ip</i>		(Optional) Global IP address.
<i>global-port</i>		(Optional) Global port.
<i>local-ip</i>		(Optional) Local IP address.
<i>local-port</i>		(Optional) Local port.
<b>outside</b>		(Optional) Clears the outside translations containing the specified <i>global</i> and <i>local</i> addresses.
<b>esp</b>		(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
<b>tcp</b>		(Optional) Clears the TCP entries from the translation table.
<b>udp</b>		(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.

Command Modes	
	EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(15)T	The <b>esp</b> keyword was added.

Usage Guidelines	
	Use this command to clear entries from the translation table before they time out.

Examples	
	The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router> show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

## clear ip nat translation

```
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
```

```
Router# show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23 171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23 171.69.1.161:23
```

## Related Commands

Command	Description
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Changes the amount of time after which NAT translations time out.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** EXEC command.

## **clear ip nhrp**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	11.0	This command was introduced.

**Usage Guidelines** This command does not clear any static (configured) IP-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

**Examples** The following example clears all dynamic entries from the NHRP cache for the interface:

```
clear ip nhrp
```

Related Commands	Command	Description
	<b>show ip nhrp</b>	Displays the NHRP cache.

# clear ip route dhcp

To remove routes from the routing table added by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent for the DHCP clients on unnumbered interfaces, use the **clear ip route dhcp** command in EXEC mode.

```
clear ip route [vrf vrf-name] dhcp [ip-address]
```

Syntax Description	Parameter	Description
	<b>vrf</b>	(Optional) VPN routing and forwarding instance (VRF).
	<i>vrf-name</i>	(Optional) Name of the VRF.
	<i>ip-address</i>	(Optional) Address about which routing information should be removed.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	12.2	This command was introduced.

**Usage Guidelines** To remove information about global routes in the routing table, use the **clear ip route dhcp** command. To remove routes in the VRF routing table, use the **clear ip route vrf vrf-name dhcp** command.

**Examples** The following example removes a route to network 55.5.5.217 from the routing table:

```
Router# clear ip route dhcp 55.5.5.217
```

Related Commands	Command	Description
	<b>show ip route dhcp</b>	Displays the routes added to the routing table by the Cisco IOS DHCP server and relay agent.



# clear ip route

To delete routes from the IP routing table, use the **clear ip route** EXEC command.

```
clear ip route {network [mask] | *}
```

Syntax Description		
	<i>network</i>	Network or subnet address to remove.
	<i>mask</i>	(Optional) Subnet address to remove.
	*	Removes all routing table entries.

**Defaults** All entries are removed.

**Command Modes** EXEC

Command History	Release	Modification
	10.0	This command was introduced.

**Examples** The following example removes a route to network 132.5.0.0 from the IP routing table:

```
clear ip route 132.5.0.0
```

# clear ip slb

To clear IP IOS SLB connections or counters, use the **clear ip slb** privileged EXEC command.

```
clear ip slb { connections [serverfarm farm-name | vserver server-name] | counters }
```

Syntax Description	connections	Clears the IP IOS SLB connection database.
	<b>serverfarm</b>	(Optional) Clears the connection database for the server farm named.
	<i>farm-name</i>	(Optional) Character string used to identify the server farm.
	<b>vserver</b>	(Optional) Clears the connection database for the virtual server named.
	<i>server-name</i>	(Optional) Character string used to identify the virtual server.
	<b>counters</b>	Clears the IP IOS SLB counters.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Examples** The following example clears the connection database of the server farm named FARM1:

```
Router# clear ip slb connections serverfarm FARM1
```

The following example clears the connection database of the virtual server named VSERVER1:

```
Router# clear ip slb connections vserver VSERVER1
```

The following example clears the IOS SLB counters:

```
Router# clear ip slb counters
```

Related Commands	Command	Description
	<b>show ip slb conns</b>	Displays information about the IOS SLB connections.
	<b>show ip slb serverfarms</b>	Displays information about the IOS SLB server farms.
	<b>show ip slb vservers</b>	Displays information about the IOS SLB virtual servers.

# clear ip snat sessions

To clear dynamic Stateful Network Address Translation (SNAT) sessions from the translation table, use the **clear ip snat sessions** command in EXEC mode.

```
clear ip snat sessions * [ip-address-peer]
```

Syntax Description	*	Removes all dynamic entries.
	<i>ip-address-peer</i>	(Optional) Removes SNAT entries of the peer translator.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	Use this command to clear entries from the translation table before they time out.
------------------	--

Examples	The following example shows the SNAT entries before and after using the <b>clear ip snat sessions</b> command:.
----------	---

```
Router# show ip snat distributed

SNAT:Mode PRIMARY
  :State READY
  :Local Address 192.168.123.2
  :Local NAT id 100
  :Peer Address 192.168.123.3
  :Peer NAT id 200
  :Mapping List 10

Router# clear ip snat sessions *
Closing TCP session to peer:192.168.123.3
Router# show ip snat distributed
```

# clear ip snat translation distributed

To clear dynamic Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation distributed** command in EXEC mode.

**clear ip snat translation distributed \***

<b>Syntax Description</b>	*	Removes all dynamic SNAT entries.
---------------------------	---	-----------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(13)T	This command was introduced.

<b>Usage Guidelines</b>	Use this command to clear entries from the translation table before they time out.
-------------------------	--

<b>Examples</b>	The following example clears all dynamic SNAT translations from the translation table: <pre>Router# clear ip snat translations distributed *</pre>
-----------------	---

# clear ip snat translation peer

To clear peer Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation peer** command in EXEC mode.

```
clear ip snat translation peer ip-address-peer [refresh]
```

Syntax Description	<i>ip-address-peer</i>	IP address of the peer translator.
	<b>refresh</b>	(Optional) Provides a fresh dump of the NAT table from the peer.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

**Usage Guidelines** Use this command to clear peer entries from the translation table before they time out.

**Examples** The following example shows the SNAT entries before and after the peer entry is cleared:

```
Router# show ip snat peer

Pro Inside global      Inside local      Outside local      Outside global
--- 192.168.25.20      192.168.122.20   ---               ---
tcp 192.168.25.20:33528 192.168.122.20:33528 192.168.24.2:21 192.168.24.2:21

Router# clear ip snat translation peer 192.168.122.20
```

# clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the **clear ip wccp** command in EXEC mode.

```
clear ip wccp { web-cache | service-number }
```

Syntax Description	web-cache	Directs the router to remove statistics for the web cache service.
	<i>service-number</i>	Directs the router to remove statistics for a specified cache service. The number can be from 0 to 99.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	11.1 CA	This command was introduced for Cisco 7200 and 7500 platforms.
	11.2 P	Support for this command was added to a variety of Cisco platforms.
	12.0(3)T	This command was expanded to be explicit about service using the <b>web-cache</b> keyword and the <i>service-number</i> argument.

**Usage Guidelines** Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics. If Cisco Cache Engines are used in your service group, the reverse proxy service is indicated by a value of 99.

**Examples** In the following example, all statistics associated with the web cache service are removed:

```
Router# clear ip wccp web-cache
```

Related Commands	Command	Description
	<b>ip wccp</b>	Directs a router to enable or disable the support for a cache engine service group.
	<b>show ip wccp</b>	Displays global statistics related to the WCCP.

# clear tcp statistics

To clear TCP statistics, use the **clear tcp statistics** command in privileged EXEC command.

**clear tcp statistics**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** Privileged EXEC

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3	This command was introduced.

---

---

**Examples** The following example clears all TCP statistics:

```
Router# clear tcp statistics
```

---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show tcp statistics</b>	Displays TCP statistics.

---

# clear time-range ipc

To clear the time-range interprocess communications (IPC) message statistics and counters between the Route Processor and the line card, use the **clear time-range ipc** command in privileged EXEC mode.

## clear time-range ipc

**Syntax Description** This command has no argument or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(2)T	This command was introduced.

**Examples** The following example clears the time-range IPC statistics and counters:

```
Router# clear time-range ipc
```

Related Commands	Command	Description
	<b>debug time-range ipc</b>	Enables debugging output for monitoring the time-range IPC messages between the Route Processor and the line card.
	<b>show time-range ipc</b>	Displays the statistics about the time-range IPC messages between the Route Processor and line card.



# client

To define which clients are allowed to use the virtual server, use the **client** SLB virtual server configuration command. You can use more than one client command to define more than one client. To remove a client definition from the IOS SLB configuration, use the **no** form of this command.

**client** *ip-address network-mask*

**no client** *ip-address network-mask*

Syntax Description	
<i>ip-address</i>	Client IP address. The default is 0.0.0.0 (all clients).
<i>network-mask</i>	Client IP network mask. The default is 0.0.0.0 (all subnetworks).

Defaults	
	The default IP address is 0.0.0.0 (all clients).
	The default network mask is 0.0.0.0 (all subnetworks).
	Taken together, the default is <b>client 0.0.0.0 0.0.0.0</b> (allows all clients on all subnetworks to use the virtual server).

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.

Usage Guidelines	
	The <i>network-mask</i> value is applied to the source IP address of incoming connections. The result must match the <i>ip-address</i> value for the client to be allowed to use the virtual server.

Examples	
	The following example allows only clients from 10.4.4.x access to the virtual server:

```
ip slb vserver PUBLIC_HTTP
client 10.4.4.0 255.255.255.0
```

Related Commands	Command	Description
	<b>show ip slb vservers</b>	Displays information about the virtual servers.
	<b>virtual</b>	Configures the virtual server attributes.

# client-identifier

To specify the unique identifier (in dotted hexadecimal notation) for a Microsoft Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** command in DHCP pool configuration mode. To delete the client identifier, use the **no** form of this command.

**client-identifier** *unique-identifier*

**no client-identifier**

<b>Syntax Description</b>	<i>unique-identifier</i>	The distinct identification of the client in dotted-hexadecimal notation, for example, 01b7.0813.8811.66.
---------------------------	--------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Usage Guidelines</b>	This command is valid for manual bindings only. Microsoft DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address b708.1388.f166 is 01b7.0813.88f1.66, where 01 represents the Ethernet media type. For a list of media type codes, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, <i>Assigned Numbers</i> .
-------------------------	--

<b>Examples</b>	The following example specifies the client identifier for MAC address 01b7.0813.8811.66 in dotted hexadecimal notation:
-----------------	---

```
client-identifier 01b7.0813.8811.66
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>hardware-address</b>	Specifies the hardware address of a DHCP client.
	<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.

# client-name

To specify the name of a DHCP client, use the **client-name** command in DHCP pool configuration mode. To remove the client name, use the **no** form of this command.

**client-name** *name*

**no client-name**

<b>Syntax Description</b>	<i>name</i>	Specifies the name of the client, using any standard ASCII character. The client name should not include the domain name. For example, the name <b>mars</b> should not be specified as <b>mars.cisco.com</b> .
---------------------------	-------------	--

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Usage Guidelines</b>	The client name should not include the domain name.
-------------------------	---

<b>Examples</b>	The following example specifies a string client1 that will be the name of the client: <code>client-name client1</code>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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.

# crypto ipsec

To enable security parameter index (SPI) matching between two Virtual Private Network (VPN) devices, use the **crypto ipsec** command on both devices in global configuration mode. To disable SPI matching, use the **no** form of this command.

**crypto ipsec spi-matching**

**no crypto ipsec spi-matching**

Syntax Description	<b>spi-matching</b>	Enables SPI matching on both endpoints.
Defaults	SPI matching in IPsec is not enabled by default.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.2(15)T	This command was introduced.
Usage Guidelines	The generation of SPIs that are predictable and symmetric is enabled. SPI matching should be used in conjunction with Network Address Translation (NAT) devices when multiple ESP connections across a NAT device is desired.	
Examples	<p>The following example enables SPI matching on the endpoint routers:</p> <pre>crypto ipsec spi-matching</pre>	
Related Commands	Command	Description
	<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
	<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
	<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
	<b>ip nat inside source</b>	Enables NAT of the inside source address.
	<b>ip nat outside source</b>	Enables NAT of the outside source address.
	<b>show ip nat statistics</b>	Displays NAT statistics.
	<b>show ip nat translations</b>	Displays active NAT translations.

## 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**

<b>Syntax Description</b>	<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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		12.0(1)T

**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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>ip dhcp pool</b>

# 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* }

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

Syntax Description	up	Time to delay the notification of an up event.
	down	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 the IOS SLB feature 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*

**no delay**

<b>Syntax Description</b>	<i>duration</i>	Delay timer duration in seconds. The valid range is from 1 to 600 seconds. The default value is 10 seconds.
---------------------------	-----------------	---

<b>Defaults</b>	The default duration is 10 seconds.
-----------------	-------------------------------------

<b>Command Modes</b>	SLB virtual server configuration
----------------------	----------------------------------

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

<b>Usage Guidelines</b>	<p>The delay timer allows out-of-sequence packets and final acknowledgments (ACKs) to be delivered after a TCP connection ends.</p> <p>Do not set this value to zero (0).</p> <p>If you are configuring a delay timer for HTTP flows, choose a low number such as 5 seconds as a starting point.</p>
-------------------------	--

<b>Examples</b>	<p>The following example specifies that the IOS SLB feature maintains TCP connection context for 30 seconds after a connection has terminated:</p>
-----------------	--

```
ip slb vserver PUBLIC_HTTP
  delay 30
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip slb vservers</b>	Displays information about the virtual servers.
	<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 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>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   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>
<b>{+   -} flag-name</b>	<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,	<p>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 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 IP 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.

Command	Description
<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>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**

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

<b>Defaults</b>	No default behavior or values.	
-----------------	--------------------------------	--

<b>Command Modes</b>	DHCP pool configuration	
----------------------	-------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Examples</b>	The following example specifies cisco.com as the domain name of the client:	
-----------------	---	--

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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>	(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.
<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 ICMP message type and code name. The possible names are found in the section “Usage Guidelines.”
<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 section “Usage Guidelines.”
<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>	(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.
<b>established</b>	(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.

**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..
<p>...no <b>fragments</b> keyword (the default behavior), and assuming all of the access-list entry information matches,</p>	<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>
<p>...the <b>fragments</b> keyword, and assuming all of the access-list entry information matches,</p>	<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 it has higher priority than the current AVF, use the **glbp forwarder preempt** command in interface configuration mode. To disable this feature, use the **no** form of this command.

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

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

<b>Syntax Description</b>	<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.

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

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		12.2(14)S
	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 AVF when its priority is higher than that of the current AVF. 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
		<b>glbp ip</b>

# 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.

Command	Description
<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

<i>group</i>	GLBP group number in the range from 0 to 1023.
<i>level</i>	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

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	
	<i>hellotime</i> : 3 seconds
	<i>holdtime</i> : 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 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		
<i>group</i>	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 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</b> <i>lower</i>	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
<b>upper</b> <i>upper</i>	(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.

# 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**

Command	Description
<b>glbp weighting</b>	Specifies the initial weighting value 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

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.

# idle

To specify the minimum amount of time for which IOS SLB maintains connection information in the absence of packet activity, use the **idle** command in virtual server configuration mode. To restore the default idle duration value, use the **no** form of this command.

**idle** *duration*

**no idle**

<b>Syntax Description</b>	<i>duration</i>	Idle connection timer duration (in seconds). Valid values range from 10 to 65535. The default is 3600 seconds (1 hour).
---------------------------	-----------------	---

<b>Defaults</b>	The default duration is 3600 seconds.
-----------------	---------------------------------------

<b>Command Modes</b>	SLB virtual server configuration
----------------------	----------------------------------

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

<b>Usage Guidelines</b>	<p>TCP connections that do not send flows or keepalives before the idle timer expires are assumed to be inactive and are reset (RST).</p> <p>If you are configuring an idle timer for HTTP flows, choose a low number such as 120 seconds as a starting point. A low number ensures that the IOS SLB connection database maintains a manageable size if problems at the server, client, or network result in a large number of connections. However, do not choose a value under 60 seconds; such a low value can reduce the efficiency of the IOS SLB feature.</p>
-------------------------	---

<b>Examples</b>	The following example instructs the IOS SLB feature to maintain connection information for an idle connection for 120 seconds:
-----------------	--

```
ip slb vserver PUBLIC_HTTP
idle 120
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip slb vservers</b>	Displays information about the virtual servers.
<b>virtual</b>	Configures the virtual server attributes.	

# import all

To import Dynamic Host Configuration Protocol (DHCP) option parameters into the DHCP Server database, use the **import all** command in DHCP pool configuration mode. To disable this feature, use the **no** form of this command.

**import all**

**no import all**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** DHCP pool configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.

**Usage Guidelines** When the **no import all** command is used, the Cisco IOS DHCP Server deletes all “imported” option parameters that were added to the specified pool in the server database. Manually configured DHCP option parameters override imported DHCP option parameters.

Imported option parameters are not part of the router configuration and are not saved in NVRAM.

**Examples** The following example allows the importing of all DHCP options for a pool named pool1:

```
ip dhcp pool pool1
 network 172.16.0.0 /16
 import all
```

Related Commands	Command	Description
	<b>ip dhcp database</b>	Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.
	<b>show ip dhcp import</b>	Displays the option parameters that were imported into the DHCP Server database.

# inservice (DFP agent)

To enable the Dynamic Feedback Protocol (DFP) agent for communication with a DFP manager, use the **inservice** command in DFP agent configuration mode. To remove the DFP agent from service, use the **no** form of this command.

**inservice**

**no inservice**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The DFP agent is inactive.

**Command Modes** DFP agent configuration

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

**Usage Guidelines** A DFP agent is inactive until both of the following conditions are met:

- The DFP agent has been enabled.
- The client subsystem has changed the DFP agent to an active state.

When you use the **no** form of this command to remove a DFP agent from service, the DFP agent closes all open connections, and no new connections are assigned.

**Examples** In the following example, the DFP agent is enabled for communication with a DFP manager:

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

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

# inservice (real server)

To enable the real server for use by the Cisco IOS SLB feature, use the **inservice** SLB real server configuration command. To remove the real server from service, use the **no** form of this command.

**inservice**

**no inservice**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** If you do not specify the **inservice** command, the real server is defined to Cisco IOS SLB but is not used.

---

**Command Modes** SLB real server configuration

---

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

---

**Examples** The following example enables the real server for use by the IOS SLB feature:

```
ip slb serverfarm PUBLIC
 real 10.10.1.1
 inservice
```

---

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.

## inservice (virtual server)

To enable the virtual server for use by the IOS SLB feature, use the **inservice** SLB virtual server configuration command. To remove the virtual server from service, use the **no** form of this command.

**inservice** [*standby group-name*]

**no inservice** [*standby group-name*]

Syntax Description	standby	(Optional) Configures the Hot Standby Router Protocol (HSRP) standby virtual server.
	<i>group-name</i>	(Optional) Specifies the HSRP group name with which the IOS SLB virtual server is associated.

**Defaults** If you do not specify the **inservice** command, the virtual server is defined to IOS SLB but is not used.

**Command Modes** SLB virtual server configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced.
	12.1(1)E	The <b>standby</b> keyword and <i>group-name</i> argument were added.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

**Examples** The following example enables the real server for use by the IOS SLB feature:

```
ip slb vserver PUBLIC_HTTP
  inservice
```

Related Commands	Command	Description
	<b>show ip slb vservers</b>	Displays information about the virtual servers.
	<b>virtual</b>	Configures the virtual server attributes.

# interval (DFP agent)

To configure a Dynamic Feedback Protocol (DFP) agent weight recalculation interval, use the **interval** command in DFP agent configuration mode. To restore the default setting, use the **no** form of this command.

**interval** *seconds*

**no interval** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Specifies the number of seconds to wait before recalculating weights for the DFP manager. Valid values range from 5 to 65535 seconds. The default interval is 10 seconds.
---------------------------	----------------	---

**Defaults** The default **interval** value is 10 seconds.

**Command Modes** DFP agent configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(8a)E	This command was introduced.

**Usage Guidelines** The DFP agent sends the new weight to the DFP manager only if the new weight is different from the old weight. If the new weight is the same as the old weight, it is not sent to the DFP manager.

**Examples** The following example shows how to configure the DFP agent to recalculate weights every 11 seconds:

```
Router(config)# ip dfp agent slb
Router(config-dfp)# interval 11
```

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



# ip access-group

To control access to an interface, use the **ip access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

**ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** }

**no ip access-group** { *access-list-number* | *access-list-name* } { **in** | **out** }

Syntax Description	
<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 199 or from 1300 to 2699.
<i>access-list-name</i>	Name of an IP access list as specified by an <b>ip access-list</b> command.
<b>in</b>	Filters on inbound packets.
<b>out</b>	Filters on outbound packets.

**Defaults** No access list is applied to the interface.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	11.2	The <i>access-list-name</i> argument was added.

**Usage Guidelines** Access lists are applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

For standard outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

If the specified access list does not exist, all packets are passed.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable input access lists on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—an SSE configured with simple access lists can still switch packets, on output only).

**Examples** The following example applies list 101 on packets outbound from Ethernet interface 0:

## ■ ip access-group

```
interface ethernet 0
 ip access-group 101 out
```

Related Commands	Command	Description
	<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-list</b>	Defines an IP access list by name.
	<b>show access-lists</b>	Displays the contents of current IP and rate-limit access lists.

# ip access-list

To define an IP access list by name, use the **ip access-list** global configuration command. To remove a named IP access list, use the **no** form of this command.

```
ip access-list {standard | extended} access-list-name
```

```
no ip access-list {standard | extended} access-list-name
```

Syntax Description		
	<b>standard</b>	Specifies a standard IP access list.
	<b>extended</b>	Specifies an extended IP access list.
	<i>access-list-name</i>	Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

**Defaults** No named IP access list is defined.

**Command Modes** Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

**Usage Guidelines** Use this command to configure a named IP access list as opposed to a numbered IP access list. This command will place the router in access-list configuration mode, where you must define the denied or permitted access conditions with the **deny** and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt you get when you enter access-list configuration mode.

Use the **ip access-group** command to apply the access list to an interface.

Named access lists are not compatible with Cisco IOS releases prior to Release 11.2.

**Examples** The following example defines a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 permit 192.5.34.0 0.0.0.255
 permit 128.88.0.0 0.0.255.255
 permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

## Related Commands

Command	Description
<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>access-list remark</b>	Writes a helpful comment (remark) for an entry in a numbered access list.
<b>deny (IP)</b>	Sets conditions for a named IP access list.
<b>ip access-group</b>	Controls access to an interface.
<b>permit (IP)</b>	Sets conditions for a named IP access list.
<b>remark</b>	Writes a helpful comment (remark) for an entry in a named IP access list.
<b>show ip access-list</b>	Displays the contents of all current IP access lists.

# ip access-list resequence

To apply sequence numbers to the access list entries in an access list, use the **ip access-list resequence** command in global configuration mode. This command does not have a **no** version.

**ip access-list resequence** *access-list-name starting-sequence-number increment*

Syntax Description		
	<i>access-list-name</i>	Name of the access list. Names cannot contain a space or quotation mark.
	<i>starting-sequence-number</i>	Access list entries will be resequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 2147483647.
	<i>increment</i>	The number by which the sequence numbers change. The default value is 10. For example, if the increment value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.

**Defaults** Disabled

**Command Modes** Global 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 allows the **permit** and **deny** entries of a specified access list to be resequenced with an initial sequence number value determined by the *starting-sequence-number* argument, and continuing in increments determined by the *increment* argument. If the highest sequence number exceeds the maximum possible sequence number, then no sequencing occurs.

For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

Exceeded maximum sequence number.

If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.

If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.

If the user enters a sequence number that is already present, the following error message is generated:

Duplicate sequence number.

If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.

Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card (LC) are in synchronization at all times.

Sequence numbers are not nvgened. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment.

This command works with named standard and extended IP access lists. Because the name of an access list can be designated as a number, numbers are acceptable as names as long as they are entered in named access list configuration mode.

### Examples

The following example resequences an access list named kmd1. The starting sequence number is 100, and the increment value is 5:

```
Router(config)# ip access-list resequence kmd1 100 5
```

### Related Commands

Command	Description
<b>deny (IP)</b>	Sets conditions under which a packet does not pass a named IP access list.
<b>permit (IP)</b>	Sets conditions under which a packet passes a named IP access list.

# ip accounting

To enable IP accounting on an interface, use the **ip accounting** command in interface configuration mode. To disable IP accounting, use the **no** form of this command.

**ip accounting** [**access-violations**] [**output-packets**]

**no ip accounting** [**access-violations**] [**output-packets**]

Syntax Description	access-violations	(Optional) Enables IP accounting with the ability to identify IP traffic that fails IP access lists.
	output-packets	(Optional) Enables IP accounting based on the IP packets output on the interface.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The <b>access-violations</b> keyword was added.

**Usage Guidelines** The **ip accounting** command records the number of bytes (IP header and data) and packets switched through the system on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis; traffic generated by the router access server or terminating in this device is not included in the accounting statistics.

If you specify the **access-violations** keyword, the **ip accounting** command provides information identifying IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists alerts you to possible attempts to breach security. The data might also indicate that you should verify IP access list configurations.

To receive a logging message on the console when an extended access list entry denies a packet access (to log violations), you must include the **log** keyword in the **access-list** (IP extended) or **access-list** (IP standard) command.

Statistics are accurate even if IP fast switching or IP access lists are being used on the interface.

IP accounting disables autonomous switching, SSE switching, and distributed switching (dCEF) on the interface. IP accounting will cause packets to be switched on the Route Switch Processor (RSP) instead of the Versatile Interface Processor (VIP), which can cause performance degradation.

**Examples** The following example enables IP accounting on Ethernet interface 0:

```
interface ethernet 0
 ip accounting
```

## Related Commands

Command	Description
<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>clear ip accounting</b>	Clears the active or checkpointed database when IP accounting is enabled.
<b>ip accounting-list</b>	Defines filters to control the hosts for which IP accounting information is kept.
<b>ip accounting-threshold</b>	Sets the maximum number of accounting entries to be created.
<b>ip accounting-transits</b>	Controls the number of transit records that are stored in the IP accounting database.
<b>show ip accounting</b>	Displays the active accounting or checkpointed database or displays access list violations.



# ip accounting mac-address

To enable IP accounting on a LAN interface based on the source and destination MAC address, use the **ip accounting mac-address** command in interface configuration mode. To disable IP accounting based on the source and destination MAC address, use the **no** form of this command.

**ip accounting mac-address** {input | output}

**no ip accounting mac-address** {input | output}

## Syntax Description

<b>input</b>	Performs accounting based on the source MAC address on received packets.
<b>output</b>	Performs accounting based on the destination MAC address on transmitted packets.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

Release	Modification
11.1CC	This command was introduced.

## Usage Guidelines

This feature is supported on Ethernet, Fast Ethernet, and FDDI interfaces.

To display the MAC accounting information, use the **show interface mac EXEC** command.

MAC address accounting provides accounting information for IP traffic based on the source and destination MAC address on LAN interfaces. This calculates the total packet and byte counts for a LAN interface that receives or sends IP packets to or from a unique MAC address. It also records a timestamp for the last packet received or sent. With MAC address accounting, you can determine how much traffic is being sent to and/or received from various peers at NAPS/peering points.

## Examples

The following example enables IP accounting based on the source and destination MAC address for received and transmitted packets:

```
interface ethernet 4/0/0
 ip accounting mac-address input
 ip accounting mac-address output
```

## Related Commands

Command	Description
<b>show interface mac</b>	Displays MAC accounting information for interfaces configured for MAC accounting.

# ip accounting precedence

To enable IP accounting on any interface based on IP precedence, use the **ip accounting precedence** command in interface configuration mode. To disable IP accounting based on IP precedence, use the **no** form of this command.

**ip accounting precedence {input | output}**

**no ip accounting precedence {input | output}**

Syntax Description	input	output
	Performs accounting based on IP precedence on received packets.	Performs accounting based on IP precedence on transmitted packets.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	11.1CC	This command was introduced.

**Usage Guidelines** To display IP precedence accounting information, use the **show interface precedence EXEC** command. The precedence accounting feature provides accounting information for IP traffic, summarized by IP precedence values. This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on IP precedence. This feature is supported on all interfaces and subinterfaces and supports CEF, dCEF, flow, and optimum switching.

**Examples** The following example enables IP accounting based on IP precedence for received and transmitted packets:

```
interface ethernet 4/0/0
 ip accounting precedence input
 ip accounting precedence output
```

Related Commands	Command	Description
	<b>show interface precedence</b>	Displays precedence accounting information for an interface configured for precedence accounting.

# ip accounting-list

To define filters to control the hosts for which IP accounting information is kept, use the **ip accounting-list** command in global configuration mode. To remove a filter definition, use the **no** form of this command.

**ip accounting-list** *ip-address wildcard*

**no ip accounting-list** *ip-address wildcard*

## Syntax Description

<i>ip-address</i>	IP address in dotted decimal format.
<i>wildcard</i>	Wildcard bits to be applied to the <i>ip-address</i> argument.

## Defaults

No filters are defined.

## Command Modes

Global configuration

## Command History

Release	Modification
10.0	This command was introduced.

## Usage Guidelines

The *wildcard* argument is a 32-bit quantity written in dotted-decimal format. Address bits corresponding to wildcard bits set to 1 are ignored in comparisons; address bits corresponding to wildcard bits set to zero are used in comparisons.

## Examples

The following example adds all hosts with IP addresses beginning with 192.31 to the list of hosts for which accounting information will be kept:

```
ip accounting-list 192.31.0.0 0.0.255.255
```

## Related Commands

Command	Description
<b>clear ip accounting</b>	Clears the active or checkpointed database when IP accounting is enabled.
<b>ip accounting</b>	Enables IP accounting on an interface.
<b>ip accounting-threshold</b>	Sets the maximum number of accounting entries to be created.
<b>ip accounting-transits</b>	Controls the number of transit records that are stored in the IP accounting database.
<b>show ip accounting</b>	Displays the active accounting or checkpointed database or displays access list violations.

# ip accounting-threshold

To set the maximum number of accounting entries to be created, use the **ip accounting-threshold** command in global configuration mode. To restore the default number of entries, use the **no** form of this command.

**ip accounting-threshold** *threshold*

**no ip accounting-threshold** *threshold*

<b>Syntax Description</b>	<i>threshold</i>	Maximum number of entries (source and destination address pairs) that the Cisco IOS software accumulates.
---------------------------	------------------	---

**Defaults** The default maximum number of accounting entries is 512 entries.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Usage Guidelines** The accounting threshold defines the maximum number of entries (source and destination address pairs) that the software accumulates, preventing IP accounting from possibly consuming all available free memory. This level of memory consumption could occur in a router that is switching traffic for many hosts. Overflows will be recorded; see the monitoring commands for display formats.

The default accounting threshold of 512 entries results in a maximum table size of 12,928 bytes. Active and checkpointed tables can reach this size independently.

**Examples** The following example sets the IP accounting threshold to 500 entries:

```
ip accounting-threshold 500
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip accounting</b>	Clears the active or checkpointed database when IP accounting is enabled.
	<b>ip accounting</b>	Enables IP accounting on an interface.
	<b>ip accounting-list</b>	Defines filters to control the hosts for which IP accounting information is kept.
	<b>ip accounting-transits</b>	Controls the number of transit records that are stored in the IP accounting database.
	<b>show ip accounting</b>	Displays the active accounting or checkpointed database or displays access list violations.

# ip accounting-transits

To control the number of transit records that are stored in the IP accounting database, use the **ip accounting-transits** command in global configuration mode. To return to the default number of records, use the **no** form of this command.

**ip accounting-transits** *count*

**no ip accounting-transits**

<b>Syntax Description</b>	<i>count</i>	Number of transit records to store in the IP accounting database.
---------------------------	--------------	---

<b>Defaults</b>	The default number of transit records that are stored in the IP accounting database is 0.
-----------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	<p>Transit entries are those that do not match any of the filters specified by <b>ip accounting-list</b> global configuration commands. If no filters are defined, no transit entries are possible.</p> <p>To maintain accurate accounting totals, the Cisco IOS software maintains two accounting databases: an active and a checkpointed database.</p>
-------------------------	--

<b>Examples</b>	The following example specifies that no more than 100 transit records are stored:
-----------------	---

```
ip accounting-transits 100
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip accounting</b>	Clears the active or checkpointed database when IP accounting is enabled.
	<b>ip accounting</b>	Enables IP accounting on an interface.
	<b>ip accounting-list</b>	Defines filters to control the hosts for which IP accounting information is kept.
	<b>ip accounting-threshold</b>	Sets the maximum number of accounting entries to be created.
	<b>show ip accounting</b>	Displays the active accounting or checkpointed database or displays access list violations.

# ip address

To set a primary or secondary IP address for an interface, use the **ip address** interface configuration command. To remove an IP address or disable IP processing, use the **no** form of this command.

**ip address** *ip-address mask* [**secondary**]

**no ip address** *ip-address mask* [**secondary**]

Syntax Description		
	<i>ip-address</i>	IP address.
	<i>mask</i>	Mask for the associated IP subnet.
	<b>secondary</b>	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

**Defaults** No IP address is defined for the interface.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines**

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

**Note**

If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

**Note**

When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

**Examples**

In the following example, 131.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
ip address 131.108.1.27 255.255.255.0
ip address 192.31.7.17 255.255.255.0 secondary
ip address 192.31.8.17 255.255.255.0 secondary
```

**Related Commands**

Command	Description
<b>bridge crb</b>	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
<b>bridge-group</b>	Assigns each network interface to a bridge group.

# ip address dhcp

To acquire an IP address on an interface from the Dynamic Host Configuration Protocol (DHCP), use the **ip address dhcp** command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

**ip address dhcp** [**client-id** *interface-name*] [**hostname** *host-name*]

**no ip address dhcp** [**client-id** *interface-name*] [**hostname** *host-name*]

## Syntax Description

<b>client-id</b>	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The <b>client-id</b> <i>interface-name</i> option sets the client identifier to the hexadecimal MAC address of the named interface.
<i>interface-name</i>	(Optional) The interface name from which the MAC address is taken.
<b>hostname</b>	(Optional) Specifies the host name.
<i>host-name</i>	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the host name entered in global configuration mode.

## Defaults

The host name is the globally configured host name of the router.  
The client identifier is an ASCII value.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	The <b>client-id</b> keyword and <i>interface-name</i> argument were added.
12.2(3)	The <b>hostname</b> keyword and <i>host-name</i> argument were added. The behavior of the <b>client-id</b> <i>interface-name</i> option changed. See the “Usage Guidelines” section for details.
12.2(8)T	The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.

## Usage Guidelines



### Note

Prior to Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.



The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific host name and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id interface-name hostname host-name** command is when *interface-name* is the Ethernet interface where the command is configured and *host-name* is the host name provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id interface** option overrides the default and forces the use of the hexadecimal MAC address of the named interface.



**Note** Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allowed the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forced the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (host name option) is included in the DISCOVER message. By default, the host name specified in option 12 will be the globally configured host name of the router. However, you can use the **ip address dhcp hostname host-name** command to place a different name in the DHCP option 12 field than the globally configured host name of the router.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. [Table 2](#) shows the possible configuration methods and the information placed in the DISCOVER message for each method.

**Table 2** Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
<b>ip address dhcp</b>	The DISCOVER message contains “cisco-mac-address -Eth1” in the client ID field. The <i>mac-address</i> is the MAC address of the Ethernet 1 interface and contains the default host name of the router in the option 12 field.
<b>ip address dhcp hostname host-name</b>	The DISCOVER message contains “cisco-mac-address -Eth1” in the client ID field. The <i>mac-address</i> is the MAC address of the Ethernet 1 interface, and contains <i>host-name</i> in the option 12 field.

**Table 2** Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
<b>ip address dhcp client-id ethernet 1</b>	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default host name of the router in the option 12 field.
<b>ip address dhcp client-id ethernet 1 hostname <i>host-name</i></b>	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains <i>host-name</i> in the option 12 field.

**Examples**

In the examples that follow, the command **ip address dhcp** is entered for the Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain “cisco-*mac-address* -Eth1” in the client-ID field, and the value *fresno* in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain “cisco-*mac-address* -Eth1” in the client-ID field, and the value *sanfran* in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp hostname sanfran
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of the Ethernet 1 interface in the client-id field, and the value *fresno* in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of the Ethernet 1 interface in the client-id field, and the value *sanfran* in the option 12 field.

```
hostname fresno
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname sanfran
```

**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.

# ip address pool (DHCP)

To enable the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IP Control Protocol (IPCP) negotiation, use the **ip address pool** command in interface configuration mode. To disable autoconfiguring of the IP address of the interface, use the **no** form of this command.

**ip address pool** *name*

**no ip address pool**

<b>Syntax Description</b>	<i>name</i>	Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in <i>name</i> .
---------------------------	-------------	---

<b>Defaults</b>	IP address pooling is disabled.
-----------------	---------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

<b>Usage Guidelines</b>	Use this command to automatically configure the IP address of a LAN interface when there are DHCP clients on the attached LAN that should be serviced by the DHCP pool on the router. The DHCP pool obtains its subnet dynamically through IPCP subnet negotiation.
-------------------------	---

<b>Examples</b>	The following example specifies that the IP address of Ethernet interface 2 will be automatically configured from the address pool named abc:
-----------------	---

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface Ethernet 2
  ip address pool abc
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip interface</b>	Displays the usability status of interfaces configured for IP.

# ip broadcast-address

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restore the default IP broadcast address, use the **no** form of this command.

**ip broadcast-address** [*ip-address*]

**no ip broadcast-address** [*ip-address*]

<b>Syntax Description</b>	<i>ip-address</i> (Optional) IP broadcast address for a network.
---------------------------	--

<b>Defaults</b>	Default address: 255.255.255.255 (all ones)
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Examples</b>	<p>The following example specifies an IP broadcast address of 0.0.0.0:</p> <pre>ip broadcast-address 0.0.0.0</pre>
-----------------	--

# ip casa

To configure the router to function as a forwarding agent, use the **ip casa** global configuration command. To disable the forwarding agent, use the **no** form of this command.

**ip casa** *control-address igmp-address*

**no ip casa**

Syntax Description		
	<i>control-address</i>	IP address of the forwarding agent side of the services manager/forwarding agent tunnel used for sending signals. This address is unique for each forwarding agent.
	<i>igmp-address</i>	IGMP address on which the forwarding agent will listen for wildcard and fixed affinities.

**Defaults** No default behavior or values.

**Command Modes** Global configuration

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

**Examples** The following example specifies the Internet address (10.10.4.1) and IGMP address (224.0.1.2) for the forwarding agent:

```
ip-casa 10.10.4.1 224.0.1.2
```

Related Commands	Command	Description
	<b>forwarding-agent</b>	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.

# ip cef traffic-statistics

To change the time interval that controls when Next Hop Resolution Protocol (NHRP) will set up or tear down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** global configuration command. To restore the default values, use the **no** form of this command.

**ip cef traffic-statistics** [**load-interval** *seconds*] [**update-rate** *seconds*]

**no ip cef traffic-statistics**

Syntax Description	
<b>load-interval</b> <i>seconds</i>	(Optional) Length of time (in 30-second increments) during which the average <i>trigger-threshold</i> and <i>teardown-threshold</i> intervals are calculated before an SVC setup or teardown action is taken. (These thresholds are configured in the <b>ip nhrp trigger-svc</b> command.) The <b>load-interval</b> range is from 30 seconds to 300 seconds, in 30-second increments. The default value is 30 seconds.
<b>update-rate</b> <i>seconds</i>	(Optional) Frequency that the port adapter sends the accounting statistics to the Route Processor (RP). When using NHRP in distributed CEF switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

Defaults	
	<b>load-interval:</b> 30 seconds
	<b>update-rate:</b> 10 seconds

Command Modes	
	Global configuration

Command History	Release	Modification
	12.0	This command was introduced.

**Usage Guidelines**

The **ip nhrp trigger-svc** command sets the threshold by which NHRP sets up and tears down a connection. The threshold is the CEF traffic load statistics. The thresholds in the **ip nhrp trigger-svc** command are measured during a sampling interval of 30 seconds, by default. To change that interval over which that threshold is determined, use the **load-interval** *seconds* option of the **ip cef traffic-statistics** command.

When NHRP is configured on a CEF switching node with a Versatile Interface Processor (VIP2) adapter, you must make sure the **update-rate** keyword is set to 5 seconds.

Other Cisco IOS features could also use the **ip cef traffic-statistics** command; this NHRP feature relies on it.

---

**Examples**

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
ip cef traffic-statistics load-interval 120
```

---

**Related Commands**

Command	Description
<b>ip nhrp trigger-svc</b>	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

---

# ip classless

At times the router might receive packets destined for a subnet of a network that has no network default route. To have the Cisco IOS software forward such packets to the best supernet route possible, use the **ip classless** global configuration command. To disable this feature, use the **no** form of this command.

**ip classless**

**no ip classless**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled

**Command Modes** Global configuration

## Command History

Release	Modification
10.0	This command was introduced.
11.3	The default behavior changed from disabled to enabled.

## Usage Guidelines

This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the Cisco IOS software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, no such subnet number is in the routing table, and there is no network default route.



### Note

If the supernet, or default route, is learned via IS-IS or OSPF, the **no ip classless** configuration command is ignored.

## Examples

The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```



# ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** global configuration command. To disable this function, use the **no** form of this command.

**ip default-gateway** *ip-address*

**no ip default-gateway** *ip-address*

<b>Syntax Description</b>	<i>ip-address</i>	IP address of the router.
---------------------------	-------------------	---------------------------

<b>Defaults</b>	Disabled
-----------------	----------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	10.0	This command was introduced.

<b>Usage Guidelines</b>	The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an Internet Control Message Protocol (ICMP) redirect message back. The ICMP redirect message indicates which local router the Cisco IOS software should use.
-------------------------	--

<b>Examples</b>	The following example defines the router on IP address 192.31.7.18 as the default router:
-----------------	---

```
ip default-gateway 192.31.7.18
```

<b>Related Commands</b>	Command	Description
	<b>ip redirects</b>	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
<b>show ip redirects</b>	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.	

# ip dfp agent

To identify a Dynamic Feedback Protocol (DFP) agent subsystem and initiate DFP agent configuration mode, use the **ip dfp agent** command in global configuration mode. To remove the DFP agent identification, use the **no** form of this command.

**ip dfp agent** *subsystem-name*

**no ip dfp agent** *subsystem-name*

<b>Syntax Description</b>	<i>subsystem-name</i>	Character string that identifies a DFP agent subsystem and enables a subsystem to send weights to a DFP manager. The <i>subsystem-name</i> argument has a 15-character limit.
---------------------------	-----------------------	---

<b>Defaults</b>	No DFP agent subsystem is defined.
-----------------	------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

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

<b>Usage Guidelines</b>	To discover the subsystem names that are available in your network, enter the <b>ip dfp agent ?</b> command.
-------------------------	--

<b>Examples</b>	The following example shows how to configure a DFP agent subsystem named slb and enter DFP agent configuration mode:
-----------------	--

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

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

# ip dhcp aaa default username

To specify the default user name for non-VRF address pools that have been configured to obtain subnets through AAA, use the **ip dhcp aaa default username** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip dhcp aaa default username** *name*

**no ip dhcp aaa default username** *name*

## Syntax Description

*name* Name of the address pool.

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The behavior for when the USERNAME attribute is sent in the AAA request was changed.

## Usage Guidelines

Address pools that are configured with the **vrf** and **origin aaa** DHCP pool configuration commands will set the USERNAME attribute in the AAA request to the specified VRF name. If the VPN ID as specified in RFC 2685 is configured for the VRF, the VPN ID will be sent instead.

Address pools that are not configured with the **vrf** command but are configured with the **origin aaa** command, will set the USERNAME attribute in the AAA request to the specified *name* in the **ip dhcp aaa default username** command.

Use the **debug aaa attribute** command to verify the value of the USERNAME attribute in the subnet request to the AAA server.

In Cisco IOS Release 12.2(8)T, if this command is not configured, no AAA subnet request from non-VRF ODAPs will be sent.

In Cisco IOS Release 12.2(15)T, if the DHCP pool is not configured with VRF and the **ip dhcp aaa default username** command is not configured, the AAA request will still be sent with the USERNAME attribute set to the DHCP pool name.

This command is not needed if all ODAPs on the VHG/PE are VRF-associated.

## Examples

The following example sets the USERNAME attribute in the AAA request to green:

```
ip dhcp aaa default username green
```

**ip dhcp aaa default username****Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug aaa attribute</b>	Verifies the value of the AAA attributes.
<b>origin</b>	Configures an address pool as an on-demand address pool.
<b>vrf</b>	Associates the on-demand address pool with a VPN routing and forwarding instance.

# ip dhcp bootp ignore

To allow the Cisco IOS DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets, use the **ip dhcp bootp ignore** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

**ip dhcp bootp ignore**

**no ip dhcp bootp ignore**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The default behavior is to service BOOTP requests.

**Command Modes** Global configuration

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

**Usage Guidelines** The Cisco IOS software can forward these ignored BOOTP request packets to another DHCP server if the **ip helper-address** interface configuration command is configured on the incoming interface. If the **ip helper-address** command is not configured, the router will drop the received BOOTP request.

**Examples** The following example shows that the router will ignore received BOOTP requests:

```
hostname Router
!
ip subnet-zero
!
ip dhcp bootp ignore
```

Related Commands	Command	Description
	ip bootp server	Enables the BOOTP service on routing devices.
	<b>ip helper-address</b>	Forwards UDP broadcasts, including BOOTP, received on an interface.

# ip dhcp class

To define a DHCP class and enter DHCP class configuration mode, use the **ip dhcp class** command in global configuration mode. To remove the class, use the **no** form of this command.

**ip dhcp class** *class-name*

**no ip dhcp class** *class-name*

<b>Syntax Description</b>	<i>class-name</i>	Name of the DHCP class.
<b>Defaults</b>	No default behavior or values.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(13)ZH	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

**Usage Guidelines** DHCP class configuration provides a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside.

**Examples** The following example defines three DHCP classes and their associated relay agent information patterns. Note that CLASS3 is considered a “match to any” class because it has no relay agent information pattern configured:

```
ip dhcp class CLASS1
  relay agent information
! Relay agent information patterns
  relay-information hex 01030a0b0c020500000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 00000000000000000000FF

ip dhcp class CLASS2
  relay agent information
! Relay agent information patterns
  relay-information hex 01040102030402020102
  relay-information hex 01040101030402020102

ip dhcp class CLASS3
  relay agent information
```

Related Commands	Command	Description
	<b>relay agent information</b>	Enters relay agent information option configuration mode.
	<b>relay-information hex</b>	Specifies a hexadecimal string for the full relay agent information option.

# ip dhcp client

To configure the DHCP client to associate any added routes with a specified track number, use the **ip dhcp client** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

**ip dhcp client route track** *number*

**no ip dhcp client route track**

<b>Syntax Description</b>	<b>route track</b> <i>number</i>	Associates a track object with the DHCP-installed static route. Valid values for the <i>number</i> argument range from 1 to 500.
---------------------------	-------------------------------------	--

<b>Defaults</b>	No routes are associated with a track number.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(2)XE	This command was introduced.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

<b>Usage Guidelines</b>	You must configure the <b>ip dhcp client</b> command before issuing the <b>ip address dhcp</b> command on an interface. The <b>ip dhcp client</b> command is checked only when an IP address is acquired from DHCP. If the <b>ip dhcp client</b> command is issued after an IP address has been acquired from DHCP, this command will not take effect until the next time the router acquires an IP address from DHCP.
-------------------------	--

<b>Examples</b>	The following example configures DHCP on an Ethernet interface and associates track object 123 with routes generated from this interface:
-----------------	---

```
interface ethernet 0/0
 ip dhcp client route track 123
 ip address dhcp
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	ip address dhcp	Acquires an IP address on an Ethernet interface from the DHCP.



# ip dhcp client class-id

To specify the class identifier, use the **ip dhcp client class-id** command in interface configuration mode. To remove the class identifier, use the **no** form of this command.

```
ip dhcp client class-id { ascii string | hex string }
```

```
no ip dhcp client class-id { ascii string | hex string }
```

Syntax Description	Parameter	Description
	<b>ascii string</b>	A unique ASCII string.
	<b>hex string</b>	A unique hexadecimal value.

**Defaults** No class identifier is specified.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.3(2)XF	This command was introduced.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

**Usage Guidelines** The **ip dhcp client class-id** command is checked only when an IP address is acquired from DHCP. If the command is issued after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been configured.

The class identifier is used by vendors to specify the type of device that is requesting an IP address. For example, docsis 1.0 can be used for a cable modem and Cisco Systems, Inc. IP Phone can be used for a Cisco IP phone.

**Examples** The following example configures a class identifier with a hexadecimal string of ABCDEF1235:

```
interface Ethernet 1
 ip dhcp client class-id hex ABCDEF1235
```

Related Commands	Command	Description
	<b>ip address dhcp</b>	Acquires an IP address on an interface from DHCP.
	<b>release dhcp</b>	Performs an immediate release of a DHCP lease for an interface.
	<b>renew dhcp</b>	Performs an immediate renewal of a DHCP lease for an interface.

# ip dhcp client client-id

To specify a client identifier and override the default client identifier, use the **ip dhcp client client-id** command in interface configuration mode. To remove the overriding of the client identifier and return to the default form, use the **no** form of this command.

**ip dhcp client client-id** { *interface-name* | **ascii string** | **hex string** }

**no ip dhcp client client-id** { *interface-name* | **ascii string** | **hex string** }

## Syntax Description

<i>interface-name</i>	The interface name from which the MAC address is taken.
<b>ascii string</b>	A unique ASCII string. The default value is <i>cisco-mac-name</i> where <i>mac</i> is the MAC address of the interface and <i>name</i> is the short form of the interface name.
<b>hex string</b>	A unique hexadecimal value.

## Defaults

The client identifier is an ASCII value in the form *cisco-mac-name* where *mac* is the MAC address of the interface and *name* is the short form of the interface name.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

## Usage Guidelines

The **ip dhcp client client-id** command is checked only when an IP address is acquired from DHCP. If the command is issued after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp EXEC** commands have been configured.

When you specify the **no** form of this command, the configuration is removed and the system returns to using the default form. It is not possible to configure the system to not include a client identifier.

## Examples

The following example shows how to configure a client identifier named test-client-id:

```
interface Ethernet 1
 ip dhcp client client-id ascii test-client-id
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip address dhcp</b>	Acquires an IP address on an interface from DHCP.
<b>release dhcp</b>	Performs an immediate release of a DHCP lease for an interface.
<b>renew dhcp</b>	Performs an immediate renewal of a DHCP lease for an interface.

# ip dhcp client hostname

To specify or modify the host name sent in the DHCP message, use the **ip dhcp client hostname** command in interface configuration mode. To remove the host name, use the **no** form of this command.

**ip dhcp client hostname** *host-name*

**no ip dhcp client hostname** *host-name*

Syntax Description	<i>host-name</i>	Name of the host.
--------------------	------------------	-------------------

Defaults	The host name is the globally configured host name of the router.
----------	---

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

Command History	Release	Modification
	12.3(2)XF	This command was introduced.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

Usage Guidelines	The <b>ip dhcp client hostname</b> command is checked only when an IP address is acquired from DHCP. If the command is issued after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the <b>ip address dhcp</b> command or the <b>release dhcp</b> and <b>renew dhcp</b> EXEC commands have been configured.
------------------	--

Examples	The following example specifies the host name of the DHCP client to hostA:
----------	--

```
interface Ethernet 1
 ip dhcp client hostname hostA
```

Related Commands	Command	Description
	<b>ip address dhcp</b>	Acquires an IP address on an interface from DHCP.
	<b>release dhcp</b>	Performs an immediate release of a DHCP lease for an interface.
	<b>renew dhcp</b>	Performs an immediate renewal of a DHCP lease for an interface.

# ip dhcp client lease

To configure the duration of the lease for an IP address that is requested from a DHCP client to a DHCP server, use the **ip dhcp client lease** command in interface configuration mode. To restore to the default value, use the **no** form of this command.

**ip dhcp client lease** *days* [*hours*] [*minutes*]

**no ip dhcp client lease**

## Syntax Description

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

## Defaults

A default lease time is not included in the DHCP DISCOVER messages sent by the client. The client accepts the lease time that the DHCP server sends.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.3(2)XF	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

## Usage Guidelines

The **ip dhcp client lease** command is checked only when an IP address is acquired from DHCP. If the command is issued after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp EXEC** commands have been configured.

## Examples

The following example shows a one-day lease:

```
ip dhcp client lease 1
```

The following example shows a one-hour lease:

```
ip dhcp client lease 0 1
```

The following example shows a one-minute lease:

```
ip dhcp client lease 0 0 1
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip address dhcp</b>	Acquires an IP address on an interface from DHCP.
<b>lease</b>	Configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client
<b>release dhcp</b>	Performs an immediate release of a DHCP lease for an interface.
<b>renew dhcp</b>	Performs an immediate renewal of a DHCP lease for an interface.

# ip dhcp client request

To configure a DHCP client to request an option from a DHCP server, use the **ip dhcp client request** command in interface configuration mode. To remove the request for an option, use the **no** form of this command.

**ip dhcp client request** *option-name*

**no ip dhcp client request** *option-name*

<b>Syntax Description</b>	<i>option-name</i>	The option name can be one of the keywords <b>tftp-server-address</b> , <b>netbios-nameserver</b> , <b>vendor-specific</b> , <b>static-route</b> , <b>domain-name</b> , <b>dns-nameserver</b> , or <b>router</b> . By default, all these options are requested.
---------------------------	--------------------	---

<b>Defaults</b>	All of the options are requested.
-----------------	-----------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(2)XF	This command was introduced.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

**Usage Guidelines** Because all options are requested, the usual form of the command is the **no** form. The options specified by the **no** form are removed from the DHCP originated address for the interface.

You can reinsert an option in the list of options requested by using the same command without the **no** keyword. Multiple options can be specified on one configuration line. However, each option will appear on a separate line in the running configuration.

The **ip dhcp client request** command is checked only when an IP address is acquired from DHCP. If the command is issued after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp** EXEC commands have been configured.

**Examples** The following example shows how to configure the DHCP client to remove the DNS name server from the options requested from the DHCP server:

```
no ip dhcp client request dns-nameserver
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip address dhcp</b>	Acquires an IP address on an interface from DHCP.
<b>release dhcp</b>	Performs an immediate release of a DHCP lease for an interface.
<b>renew dhcp</b>	Performs an immediate renewal of a DHCP lease for an interface.



# ip dhcp conflict logging

To enable conflict logging on a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp conflict logging** command in global configuration mode. To disable conflict logging, use the **no** form of this command.

**ip dhcp conflict logging**

**no ip dhcp conflict logging**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Conflict logging is enabled.

**Command Modes** Global configuration

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

**Usage Guidelines** We recommend using a DHCP server database agent to store automatic bindings. If you decide not to use a DHCP Server database agent to store automatic bindings, use the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the Cisco IOS DHCP server records DHCP address conflicts in a log file.

**Examples** The following example disables the recording of DHCP address conflicts:

```
no ip dhcp conflict logging
```

Related Commands	Command	Description
	<b>clear ip dhcp conflict</b>	Clears an address conflict from the Cisco IOS DHCP server database.
	<b>ip dhcp database</b>	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.
	<b>show ip dhcp conflict</b>	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

# ip dhcp database

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent to save automatic bindings on a remote host called a database agent, use the **ip dhcp database** command in global configuration mode. To remove the database agent, use the **no** form of this command.

**ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*]

**no ip dhcp database** *url*

<b>Syntax Description</b>	<i>url</i>	Specifies the remote file used to store the automatic bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> <li>• tftp://host/filename</li> <li>• ftp://user:password@host/filename</li> <li>• rcp://user@host/filename</li> </ul>
	<b>timeout</b> <i>seconds</i>	(Optional) Specifies how long (in seconds) the DHCP Server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted. By default, DHCP waits 300 seconds (5 minutes) before aborting a database transfer. Infinity is defined as 0 seconds.
	<b>write-delay</b> <i>seconds</i>	(Optional) Specifies how soon the DHCP server should send database updates. By default, DHCP waits 300 seconds (5 minutes) before sending database changes. The minimum delay is 60 seconds.

**Defaults** DHCP waits 300 seconds for both a write delay and a timeout.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

**Usage Guidelines** The administrator may configure multiple database agents. Bindings are transferred by using FTP, Trivial File Transport Protocol (TFTP), or remote copy protocol (rcp).  
The DHCP relay agent can save route information to the same database agents to ensure recovery after reloads.

**Examples** The following example specifies the DHCP database transfer timeout value as 80 seconds:

```
ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80
```

The following example specifies the DHCP database update delay value as 100 seconds:

```
ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100
```

---

**Related Commands**

Command	Description
<b>show ip dhcp database</b>	Displays Cisco IOS DHCP Server database agent information.

---

# ip dhcp excluded-address

To specify IP addresses that a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server should not assign to DHCP clients, use the **ip dhcp excluded-address** command in global configuration mode. To remove the excluded IP addresses, use the **no** form of this command.

**ip dhcp excluded-address** *low-address* [*high-address*]

**no ip dhcp excluded-address** *low-address* [*high-address*]

Syntax Description	<i>low-address</i>	The excluded IP address, or first IP address in an excluded address range.
	<i>high-address</i>	(Optional) The last IP address in the excluded address range.

**Defaults** All IP pool addresses are assignable.

**Command Modes** Global configuration

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

**Usage Guidelines** The DHCP Server assumes that all pool addresses may be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

**Examples** The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199:

```
ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

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.
	<b>network (DHCP)</b>	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP Server.

# ip dhcp limit lease per interface

To limit the number of leases offered to (DHCP) clients behind an ATM routed bridge encapsulation (RBE) unnumbered or serial unnumbered interface, use the **ip dhcp limit lease per interface** command in global configuration mode. To remove the restriction on the number of leases, use the **no** form of the command.

**ip dhcp limit lease per interface** *lease-limit*

**no ip dhcp limit lease per interface** *lease-limit*

<b>Syntax Description</b>	<i>lease-limit</i>	Number of leases allowed.
---------------------------	--------------------	---------------------------

<b>Defaults</b>	This functionality is disabled	
-----------------	--------------------------------	--

<b>Command Modes</b>	Global configuration	
----------------------	----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(2)T	This command was introduced.

<b>Usage Guidelines</b>	This command is not supported on numbered interfaces. The lease limit can be applied only to ATM with RBE unnumbered interfaces or serial unnumbered interfaces.	
-------------------------	--	--

<b>Examples</b>	<p>The following example allows three DHCP clients to receive IP addresses. If a fourth DHCP client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server.</p> <pre>ip dhcp limit lease per interface 3</pre>	
-----------------	---	--

# ip dhcp limited-broadcast-address

To override a configured network broadcast and have the DHCP server and relay agent send an all networks, all nodes broadcast to a DHCP client, use the **ip dhcp limited-broadcast-address** global configuration command. To disable this functionality, use the **no** form of this command.

**ip dhcp limited-broadcast-address**

**no ip dhcp limited-broadcast-address**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Default broadcast address: 255.255.255.255 (all ones)

**Command Modes** Global configuration

Command History	Release	Modification
	12.1	This command was introduced.

**Usage Guidelines** When a DHCP client sets the broadcast bit in the DHCP packet, the DHCP server and relay agent send DHCP messages to clients using the all ones broadcast address (255.255.255.255). If the **ip broadcast-address** interface configuration command has been configured to send a network broadcast, the all ones broadcast set by DHCP is overridden. To remedy this situation, use the **ip dhcp limited-broadcast-address** command to ensure that a configured network broadcast does not override the default DHCP behavior.

Some DHCP clients can only accept an all ones broadcast and may not be able to acquire a DHCP address unless this command is configured on the router interface connected to the client.

**Examples** The following example configures DHCP to override any network broadcast:

```
ip dhcp limited-broadcast-address
```

Related Commands	Command	Description
	<b>ip broadcast-address</b>	Defines a broadcast address for an interface.

## ip dhcp ping packets

To specify the number of packets a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server sends to a pool address as part of a ping operation, use the **ip dhcp ping packets** command in global configuration mode. To prevent the server from pinging pool addresses, use the **no** form of this command.

**ip dhcp ping packets** *number*

**no ip dhcp ping packets**

<b>Syntax Description</b>	<i>number</i>	The number of ping packets that are sent before the address is assigned to a requesting client. The default value is two packets.
---------------------------	---------------	---

<b>Defaults</b>	Two packets
-----------------	-------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

**Usage Guidelines** The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Setting the *number* argument to a value of 0 completely turns off DHCP server ping operation .

**Examples** The following example specifies five ping attempts by the DHCP server before ceasing any further ping attempts:

```
ip dhcp ping packets 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip dhcp conflict</b>	Clears an address conflict from the Cisco IOS DHCP server database.
	<b>ip dhcp ping timeout</b>	Specifies how long a Cisco IOS DHCP Server waits for a ping reply from an address pool.
	<b>show ip dhcp conflict</b>	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

# ip dhcp ping timeout

To specify how long a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server waits for a ping reply from an address pool, use the **ip dhcp ping timeout** command in global configuration mode. To restore the default number of milliseconds (500) of the timeout, use the **no** form of this command.

**ip dhcp ping timeout** *milliseconds*

**no ip dhcp ping timeout**

<b>Syntax Description</b>	<i>milliseconds</i>	The amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The maximum timeout is 10000 milliseconds (10 seconds). The default timeout is 500 milliseconds.
---------------------------	---------------------	---

<b>Defaults</b>	500 milliseconds
-----------------	------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Usage Guidelines</b>	This command specifies how long to wait for a ping reply (in milliseconds).
-------------------------	---

**Examples** The following example specifies that the DHCP Server will wait 800 milliseconds for a ping reply before considering the ping a failure:

```
ip dhcp ping timeout 800
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip dhcp conflict</b>	Clears an address conflict from the Cisco IOS DHCP Server database.
	<b>ip dhcp ping timeout</b>	Specifies the number of packets a Cisco IOS DHCP Server sends to a pool address as part of a ping operation.
	<b>show ip dhcp conflict</b>	Displays address conflicts found by a Cisco IOS DHCP Server when addresses are offered to the client.



# ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** command in global configuration mode. To remove the address pool, use the **no** form of this command.

**ip dhcp pool** *name*

**no ip dhcp pool** *name*

<b>Syntax Description</b>	<i>name</i>	Name of the pool. Can either be a symbolic string (such as engineering) or an integer (such as 0).
<b>Defaults</b>	DHCP address pools are not configured.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.
<b>Usage Guidelines</b>	During execution of this command, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.	
<b>Examples</b>	The following example configures pool1 as the DHCP address pool: <pre>ip dhcp pool pool1</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>host</b>	Specifies the IP address and network mask for a manual binding to a DHCP client.
	<b>ip dhcp excluded-address</b>	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
	<b>network (DHCP)</b>	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

# ip dhcp relay forward spanning-tree

To set the gateway address (giaddr) field in the DHCP packet before forwarding to spanning-tree interfaces, use the **ip dhcp relay forward spanning-tree** command in global configuration mode. To disable this functionality, use the **no** form of this command.

**ip dhcp relay forward spanning-tree**

**no ip dhcp relay forward spanning-tree**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** Global configuration

## Command History

Release	Modification
12.1	This command was introduced.

## Usage Guidelines

Prior to Cisco IOS Release 12.1, when the **ip forward-protocol spanning-tree any-local-broadcast** command was configured, DHCP broadcasts were forwarded to all spanning-tree enabled interfaces after setting the giaddr field in the DHCP packet.

The behavior of the DHCP relay agent was modified in release 12.1 such that the DHCP broadcasts were still forwarded to all spanning-tree enabled interfaces but the giaddr field was not set on the packets. This behavior can cause problems in a network because the DHCP server uses the giaddr field to properly allocate addresses when the client is not in the local network.

Use the **ip dhcp relay forward spanning-tree** command to set the giaddr to the IP address of the incoming interface before forwarding DHCP broadcasts to spanning-tree enabled interfaces.

The **ip forward-protocol udp** command is enabled by default and automatically determines that BOOTP client and server datagrams (ports 67 and 68) should be forwarded. This forwarding results in another packet sent to spanning-tree enabled interfaces without the giaddr field set. To avoid these duplicate packets, use the **no ip forward-protocol udp bootpc** and **no ip forward-protocol udp bootps** commands.

## Examples

In the following example, the giaddr field in the DHCP packet will be set to the IP address of the incoming interface before forwarding to spanning-tree enabled interfaces:

```
ip dhcp relay forward spanning-tree
ip forward-protocol spanning-tree any-local-broadcast
```

Related Commands	Command	Description
	<b>ip forward-protocol</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets
	<b>ip forward-protocol spanning-tree</b>	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

# ip dhcp relay information check

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server to validate the relay agent information option in forwarded BOOTREPLY messages, use the **ip dhcp relay information check** global configuration command. To disable an information check, use the **no** form of this command.

**ip dhcp relay information check**

**no ip dhcp relay information check**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The DHCP server checks relay information. Invalid messages are dropped.

**Command Modes** Global configuration

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

**Usage Guidelines** This command is used by cable access router termination systems. By default, DHCP checks relay information. Invalid messages are dropped.

**Examples** The following example configures the DHCP Server to check that the relay agent information option in forwarded BOOTREPLY messages is valid:

```
ip dhcp relay information check
```

Related Commands	Command	Description
	<b>ip dhcp relay information option</b>	Configures a Cisco IOS DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.
	<b>ip dhcp relay information policy</b>	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).

# ip dhcp relay information option

To enable the system to insert the Dynamic Host Configuration Protocol (DHCP) relay agent information option in forwarded BOOTREQUEST messages to a Cisco IOS DHCP server, use the **ip dhcp relay information option** command in global configuration mode. To disable inserting relay information into forwarded BOOTREQUEST messages, use the **no** form of this command.

**ip dhcp relay information option [vpn]**

**no ip dhcp relay information option [vpn]**

<b>Syntax Description</b>	<b>vpn</b> (Optional) Virtual Private Network.
---------------------------	--

<b>Defaults</b>	The DHCP server does not insert relay information.
-----------------	--

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.
	12.2(4)B	The <b>vpn</b> keyword was added.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

<b>Usage Guidelines</b>	<p>This command is used by cable access router termination systems. This functionality enables a DHCP server to identify the user (cable access router) sending the request and initiate appropriate action based on this information. By default, DHCP does not insert relay information.</p>
-------------------------	--

The **ip dhcp relay information option** command automatically adds the circuit identifier suboption and the remote ID suboption to the DHCP relay agent information option (also called option 82).

The **vpn** optional keyword should be used only when the DHCP server allocates addresses based on VPN identification suboptions.

The **ip dhcp relay information option vpn** command adds the following VPN-related suboptions into the relay agent information option when DHCP broadcasts are forwarded by the relay agent from clients to a DHCP server:

- **VPN identifier**—Contains the VPN ID if configured or the VRF name if configured on the interface (VPN ID takes precedence over VRF name).
- **Subnet selection**—Contains the incoming interface subnet address.
- **Server identifier override**—Contains the incoming interface IP address.

After these suboptions are successfully added, the gateway address is set to the outgoing interface of the router toward the DHCP server IP address configured using the **ip helper-address** interface configuration command.

If only the **ip dhcp relay information option vpn** command is configured, the VPN identifier, subnet selection, and server identifier override suboptions are added to the relay information option. Note that the circuit identifier suboption and the remote ID suboption are not added to the relay information option. However, if both the **ip dhcp relay information option** command and the **ip dhcp relay information option vpn** command are configured, all five suboptions are added to the relay agent information option.

When the packets are returned from the DHCP server, option 82 is removed before the reply is forwarded to the client.

Even if the **vpn** option is specified, the VPN suboptions are added only to those DHCP or BOOTP broadcasts picked up by the interface configured with a VRF name or VPN ID.

For clients from unnumbered ATM or serial interfaces, when this command is enabled, the VPN identifier suboption will contain the VRF name of the unnumbered interface.

Subnet selection and server identifier override suboptions are added from the IP address of the interface that the unnumbered interface is configured to borrow its IP address from. The client host route will be added on the respective VRF routing tables.

If the **ip dhcp smart-relay** global configuration command is enabled, then the server identifier override and subnet selection suboptions will use the secondary IP address of the incoming interface when the same client retransmits more than three DHCP DISCOVER packets (for both numbered and unnumbered interfaces).

## Examples

The following example configures a DHCP server to insert the DHCP relay agent information option, including VPN suboptions, in forwarded BOOTREQUEST messages. In this example, the circuit identifier suboption and the remote ID suboption are not included in the relay information option:

```
ip dhcp relay information option vpn
```

The following example configures a DHCP server to insert the DHCP relay agent information option, including VPN suboptions, the circuit identifier suboption, and the remote ID suboption, in forwarded BOOTREQUEST messages:

```
ip dhcp relay information option vpn
ip dhcp relay information option
```

## Related Commands

Command	Description
<b>ip dhcp relay information check</b>	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
<b>ip dhcp relay information policy</b>	Configures the information reforwarding policy of a DHCP relay agent (what a DHCP relay agent should do if a message already contains relay information).
<b>ip dhcp smart-relay</b>	Allows the Cisco IOS DHCP relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server
<b>ip helper-address</b>	Forwards UDP broadcasts, including BOOTP, received on an interface.

# ip dhcp relay information policy

To configure the information reforwarding policy for a Dynamic Host Configuration Protocol (DHCP) relay agent (what a relay agent should do if a message already contains relay information), use the **ip dhcp relay information policy** command in global configuration . To restore the default relay information policy, use the **no** form of this command.

```
ip dhcp relay information policy {drop | keep | replace}
```

```
no ip dhcp relay information policy
```

Syntax Description	drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present.
	keep	Indicates that existing information is left unchanged on the DHCP relay agent.
	replace	Indicates that existing information is overwritten on the DHCP relay agent.

**Defaults** The DHCP server replaces existing relay information.

**Command Modes** Global configuration

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

**Usage Guidelines** This command is used by cable access router termination systems. A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced.

**Examples** The following examples configure a DHCP relay agent to drop messages with existing relay information, keep existing information, and replace existing information:

```
ip dhcp relay information policy drop
```

```
ip dhcp relay information policy keep
```

```
ip dhcp relay information policy replace
```

Related Commands	Command	Description
	<b>ip dhcp relay information check</b>	Configures a Cisco IOS DHCP Server to validate the relay agent information option in forwarded BOOTREPLY messages.
	<b>ip dhcp relay information option</b>	Configures a Cisco IOS DHCP Server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages.

# ip dhcp relay information trust-all

To configure all interfaces on a router as trusted sources of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trust-all** command in global configuration mode. To restore the interfaces to their default behavior, use the **no** form of the command.

**ip dhcp relay information trust-all**

**no ip dhcp relay information trust-all**

**Syntax Description** This command has no arguments or keywords.

**Defaults** All interfaces on the router are considered untrusted.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2	This command was introduced.

**Usage Guidelines** By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trust-all** command is configured globally, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

**Examples** In the following example, all interfaces on the router are configured as a trusted source for relay agent information:

```
ip dhcp relay information trust-all
```

Related Commands	Command	Description
	<b>ip helper-address</b>	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
	<b>show ip dhcp relay information trusted-sources</b>	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.



# ip dhcp relay information trusted

To configure an interface as a trusted source of the Dynamic Host Configuration Protocol (DHCP) relay agent information option, use the **ip dhcp relay information trusted** command in interface configuration mode. To restore the interface to the default behavior, use the **no** form of the command.

**ip dhcp relay information trusted**

**no ip dhcp relay information trusted**

## Syntax Description

This command has no arguments or keywords.

## Defaults

All interfaces on the router are considered untrusted.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.2	This command was introduced.

## Usage Guidelines

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the Cisco IOS DHCP relay agent will discard the packet. If the **ip dhcp relay information trusted** command is configured on an interface, the Cisco IOS DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the **ip helper-address** command as in normal DHCP relay operation.

## Examples

In the following example, interface Ethernet 1 is configured as a trusted source for the relay agent information:

```
interface ethernet 1
 ip dhcp relay information trusted
```

## Related Commands

Command	Description
<b>ip helper-address</b>	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.
<b>show ip dhcp relay information trusted-sources</b>	Displays all interfaces on the router that are configured as a trusted source for the DHCP relay agent information option.

# ip dhcp smart-relay

To allow the Cisco IOS Dynamic Host Configuration Protocol (DHCP) relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server, use the **ip dhcp smart-relay** global configuration command. To disable this smart-relay functionality and restore the default behavior, use the **no** form of this command.

**ip dhcp smart-relay**

**no ip dhcp smart-relay**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Release	Modification
12.1	This command was introduced.

---



---

**Usage Guidelines** The DHCP relay agent attempts to forward the primary address as the gateway address three times. After three attempts and no response, the relay agent automatically switches to secondary addresses.

---

**Examples** The following example enables the DHCP relay agent to automatically switch to secondary address pools:

```
ip dhcp smart-relay
```

# ip dhcp use class

To control whether the Cisco IOS DHCP server uses DHCP classes during address allocation, use the **ip dhcp use class** command in global configuration mode. To disable the use of DHCP classes during address allocation, use the **no** form of this command.

**ip dhcp use class**

**no ip dhcp use class**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** This command is enabled by default.

---

**Command Modes** Global configuration

---

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

---

---

**Usage Guidelines** When you use the **no ip dhcp use class** command, the DHCP class configuration is not deleted.

---

**Examples** The following example shows the DHCP server configured to use the relay agent information option during address allocation:

```
ip dhcp use class
```

# ip dhcp-client broadcast-flag

To configure the Cisco IOS Dynamic Host Configuration (DHCP) client to set the broadcast flag, use the **ip dhcp-client broadcast-flag** command in global configuration mode. To disable this feature, use the **no** form of this command.

**ip dhcp-client broadcast-flag**

**no dhcp-client broadcast-flag**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The broadcast flag is on.

**Command Modes** Global configuration

Command History	Release	Modification
	12.2	This command was introduced.

**Usage Guidelines** Use this command to set the broadcast flag to 1 or 0 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP Server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If you enter **no ip dhcp-client broadcast-flag**, the broadcast flag is set to 0 and the DHCP Server unicasts the reply packets to the client with the offered IP address.

The Cisco IOS DHCP client can receive both broadcast and unicast offers from the DHCP Server.

**Examples** The following example sets the broadcast flag on:

```
Router(config)# ip dhcp-client broadcast-flag
```

Related Commands	Command	Description
	<b>ip address dhcp</b>	Acquires an IP address on an interface via DHCP.
	<b>service dhcp</b>	Enables DHCP server and relay functions.

# ip dhcp-client default-router distance

To configure a default DHCP administrative distance for clients, use the **ip dhcp-client default-router distance** command in global configuration mode. To return to the default of 254, use the **no** form of this command.

**ip dhcp-client default-router distance** *value*

**no ip dhcp-client default-router distance** *value*

<b>Syntax Description</b>	<b>distance</b>	DHCP administrative distance. The <i>value</i> argument sets the default distance. The range is from 1 to 255.
---------------------------	-----------------	--

<b>Defaults</b>	254
-----------------	-----

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2	This command was introduced.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

**Examples** The following example shows how to configure the default administrative distance to be 25:

```
ip dhcp-client default-router distance 25
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>debug dhcp client</b>	Displays debugging information about the DHCP client activities and monitors the status of DHCP packets.
	<b>show ip route dhcp</b>	Displays the routes added to the routing table by the DHCP server and relay agent.

# ip dhcp-client network-discovery

To control the sending of Dynamic Host Configuration Protocol (DHCP) Inform and Discover messages, use the **ip dhcp-client network-discovery** command in global configuration mode. To change or disable DHCP message control, use the **no** form of this command.

**ip dhcp-client network-discovery informs** *number-of-messages* **discovers** *number-of-messages*  
**period** *seconds*

**no ip dhcp-client network-discovery informs** *number-of-messages* **discovers** *number-of-messages*  
**period** *seconds*

## Syntax Description

**informs** *number-of-messages* Number of DHCP Inform messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.

**discovers** *number-of-messages* Number of DHCP Discover messages. Valid choices are 0, 1, or 2 messages. Default is 0 messages.

**period** *seconds* Timeout period for retransmission of DHCP Inform and Discover messages. Valid periods are from 3 to 15 seconds. Default is 15 seconds.

## Defaults

0 DHCP Inform and Discover messages (network discovery is disabled when both the **informs** and **discovers** keywords are set to 0); 15-second timeout period.

## Command Modes

Global configuration

## Command History

Release	Modification
12.2	This command was introduced.

## Usage Guidelines

The **ip dhcp-client network-discovery** command allows peer routers to dynamically discover Domain Name System (DNS) and NetBIOS name server information configured on a DHCP server using PPP IP Control Protocol (IPCP) extensions. Setting the number of DHCP Inform or Discover messages to 1 or 2 determines how many times the system sends a DHCP Inform or Discover message before stopping network discovery, as follows:

- When the number of DHCP Inform messages is set to 1, once the first Inform messages is sent the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends a DHCP Discover message when the number of Discover messages is not set to 0. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

- When the number of DHCP Inform messages is set to 2, once the first Inform message is sent, the system waits for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of the timeout period, the system sends another DHCP Inform message. If the number of Discover messages is set to 1, network discovery stops. If the number of Discover messages is set to 2, the system waits again for a response from the DHCP server for the specified timeout period. If there is no response from the DHCP server by the end of this second timeout period, the system sends a second DHCP Discover message and stops network discovery.

Network discovery also stops when the DHCP server responds to DHCP Inform and Discover messages before the configured number of messages and timeout period are exceeded.

Setting the number of messages to 0 disables sending of DHCP Inform and Discover messages, and is the same as entering the **no ip dhcp-client network-discovery** command. When the **ip dhcp-client network-discovery** command is disabled, the system falls back to the static configurations made using the **async-bootp dns-server** and **async-bootp nb-server** global configuration commands or, as a last resort, to a DNS server address assigned with the **ip name-server** command.

### Examples

The following example sets two DHCP Inform and Discovery messages and a timeout period of 12 seconds:

```
ip dhcp-client network-discovery informs 2 discovers 2 period 12
```

### Related Commands

Command	Description
<b>async-bootp</b>	Configures extended BOOTP requests for asynchronous interfaces as defined in RFC 1084.
<b>ip dhcp-server</b>	Specifies which DHCP servers to use on a network, and specifies the IP address of one or more DHCP servers available on the network.
<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.

# ip dhcp-server

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, or to specify the IP address of one or more DHCP servers available on the network, use the **ip dhcp-server** command in global configuration mode. To remove a DHCP server IP address, use the **no** form of this command.

**ip dhcp-server** [*ip-address* | *name*]

**no ip dhcp-server** [*ip-address* | *name*]

## Syntax Description

<i>ip-address</i>	(Optional) IP address of a DHCP server.
<i>name</i>	(Optional) Name of a DHCP server.

## Defaults

The IP limited broadcast address of 255.255.255.255 is used for transactions if no DHCP server is specified. This default allows automatic detection of DHCP servers.

## Command Modes

Global configuration

## Command History

Release	Modification
11.0	This command was introduced.

## Usage Guidelines

A DHCP server temporarily allocates network addresses to clients through the access server on an as-needed basis. While the client is active, the address is automatically renewed in a minimum of 20-minute increments. When the user terminates the session, the interface connection is terminated so that network resources can be quickly reused. You can specify up to ten servers on the network.

In normal situations, if a SLIP or PPP session fails (for example, if a modem line disconnects), the allocated address will be reserved temporarily to preserve the same IP address for the client when dialed back into the server. This way, the session that was accidentally terminated can often be resumed.

To use the DHCP proxy-client feature, enable your access server to be a proxy-client on asynchronous interfaces by using the **ip address-pool dhcp-proxy-client** command. If you want to specify which DHCP servers are used on your network, use the **ip dhcp-server** command to define up to ten specific DHCP servers.



### Note

To facilitate transmission, configure intermediary routers (or access servers with router functionality) to use an IP helper address whenever the DHCP server is not on the local LAN and the access server is using broadcasts to interact with the DHCP server. Refer to the chapters about configuring IP addressing in the *Cisco IOS IP Configuration Guide*.

The **ip address-pool dhcp-proxy-client** command initializes proxy-client status to all interfaces defined as asynchronous on the access server. To selectively disable proxy-client status on a single asynchronous interface, use the **no peer default ip address** interface command.



---

**Examples**

The following command specifies a DHCP server with the IP address of 172.24.13.81:

```
ip dhcp-server 172.24.13.81
```

---

**Related Commands**

Command	Description
<b>ip address-pool</b>	Enables an address pooling mechanism used to supply IP addresses to dial-in asynchronous, synchronous, or ISDN point-to-point interfaces.
<b>ip helper-address</b>	Forwards UDP broadcasts, including BOOTP, received on an interface.
<b>peer default ip address</b>	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
<b>show cot dsp</b>	Displays information about the COT DSP configuration or current status.

# ip directed-broadcast

To enable the translation of a directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

**ip directed-broadcast** [*access-list-number*] | [*extended access-list-number*]

**no ip directed-broadcast** [*access-list-number*] | [*extended access-list-number*]

Syntax Description		
<i>access-list-number</i>	(Optional) Standard access list number in the range from 1 to 199. If specified, a broadcast must pass the access list to be forwarded.	
<i>extended access-list-number</i>	(Optional) Extended access list number in the range from 1300 to 2699.	

**Defaults** Disabled; all IP directed broadcasts are dropped.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0	The default behavior changed to directed broadcasts being dropped.

**Usage Guidelines** An IP directed broadcast is an IP packet whose destination address is a valid broadcast address for some IP subnet, but which originates from a node that is not itself part of that destination subnet.

A router that is not directly connected to its destination subnet forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that subnet. When a directed broadcast packet reaches a router that is directly connected to its destination subnet, that packet is “exploded” as a broadcast on the destination subnet. The destination address in the IP header of the packet is rewritten to the configured IP broadcast address for the subnet, and the packet is sent as a link-layer broadcast.

The **ip directed-broadcast** interface command controls the explosion of directed broadcasts when they reach their target subnets. The command affects only the final transmission of the directed broadcast on its ultimate destination subnet. It does not affect the transit unicast routing of IP directed broadcasts.

If **directed broadcast** is enabled for an interface, incoming IP packets whose addresses identify them as directed broadcasts intended for the subnet to which that interface is attached will be exploded as broadcasts on that subnet. If an access list has been configured with the **ip directed-broadcast** command, only directed broadcasts that are permitted by the access list in question will be forwarded; all other directed broadcasts destined for the interface subnet will be dropped.

If the **no ip directed-broadcast** command has been configured for an interface, directed broadcasts destined for the subnet to which that interface is attached will be dropped, rather than being broadcast.

**Note**

Because directed broadcasts, and particularly Internet Control Message Protocol (ICMP) directed broadcasts, have been abused by malicious persons, we recommend that security-conscious users disable the **ip directed-broadcast** command on any interface where directed broadcasts are not needed and that they use access lists to limit the number of exploded packets.

**Examples**

The following example enables forwarding of IP directed broadcasts on Ethernet interface 0:

```
interface ethernet 0
 ip directed-broadcast
```

**Related Commands**

Command	Description
<b>ip forward-protocol</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

## ip dns spoofing

To enable Domain Name System (DNS) spoofing, use the **ip dns spoofing** command in global configuration mode. To disable DNS spoofing, use the **no** form of this command.

**ip dns spoofing** [*ip-address*]

**no ip dns spoofing** [*ip-address*]

<b>Syntax Description</b>	<i>ip-address</i> (Optional) IP address used in replies to DNS queries.				
<b>Defaults</b>	No default behavior or values				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.3(2)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.3(2)T	This command was introduced.
Release	Modification				
12.3(2)T	This command was introduced.				

**Usage Guidelines** DNS spoofing allows a router to act as a proxy DNS server and “spoof” replies to any DNS queries using either the configured IP address in the **ip dns spoofing** *ip-address* command or the IP address of the incoming interface for the query. This functionality is useful for devices where the interface toward the ISP is not up. Once the interface to the ISP is up, the router forwards DNS queries to the real DNS servers.

The router will respond to the DNS query with the configured IP address when queried for any host name other than its own but will respond to the DNS query with the IP address of the incoming interface when queried for its own host name.

The host name used in the DNS query is defined as the exact configured host name of the router specified by the **hostname** *name* command, with no default domain appended. For example, in the following configuration:

```
ip domain name cisco.com
hostname sandbox
```

The system would respond with a DNS spoofing reply if queried for “sandbox” but not for “sandbox.cisco.com”.

**Examples** In the following example, the router will respond to a DNS query with an IP address of 192.168.15.1:

```
ip dns spoofing 192.168.15.1
```

# ip domain list

To define a list of default domain names to complete unqualified host names, use the **ip domain list** command in global configuration mode. To delete a name from a list, use the **no** form of this command.

**ip domain list** *name*

**no ip domain list** *name*

<b>Syntax Description</b>	<i>name</i>	Domain name. Do not include the initial period that separates an unqualified name from the domain name.
---------------------------	-------------	---

<b>Defaults</b>	No domain names are defined.
-----------------	------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
12.2	The syntax of the command changed from <b>ip domain-list</b> to <b>ip domain list</b> .	

**Usage Guidelines**

If there is no domain list, the domain name that you specified with the **ip domain name** global configuration command is used. If there is a domain list, the default domain name is not used. The **ip domain list** command is similar to the **ip domain name** command, except that with the **ip domain list** command you can define a list of domains, each to be tried in turn.

The Cisco IOS software will still accept the previous version of the command, **ip domain-list**.

**Examples**

The following example adds several domain names to a list:

```
ip domain list company.com
ip domain list school.edu
```

The following example adds a name to and then deletes a name from the list:

```
ip domain list school.edu
no ip domain list school.edu
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip domain list</b>	Defines a list of default domain names to complete unqualified host names.
	<b>ip domain lookup</b>	Enables the IP DNS-based host name-to-address translation.
	<b>ip domain retry</b>	Specifies the number of times to retry sending DNS queries.

Command	Description
<b>ip domain timeout</b>	Specifies the amount of time to wait for a response to a DNS query.
<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.

# ip domain lookup

To enable the IP Domain Naming System (DNS)-based host name-to-address translation, use the **ip domain lookup** command in global configuration mode. To disable the DNS, use the **no** form of this command.

**ip domain lookup**

**no ip domain lookup**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled

**Command Modes** Global configuration

Release	Modification
10.0	This command was introduced.
12.2	The syntax of the command changed from <b>ip domain-lookup</b> to <b>ip domain lookup</b> .

**Usage Guidelines** The Cisco IOS software will still accept the previous version of the command, which is **ip domain-lookup**.

**Examples** The following example enables the IP DNS-based host name-to-address translation:

```
ip domain lookup
```

Command	Description
<b>ip domain list</b>	Defines a list of default domain names to complete unqualified host names.
<b>ip domain lookup</b>	Enables the IP DNS-based host name-to-address translation.
<b>ip domain retry</b>	Specifies the number of times to retry sending DNS queries.
<b>ip domain timeout</b>	Specifies the amount of time to wait for a response to a DNS query.
<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.

# ip domain name

To define a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name), use the **ip domain name** command in global configuration mode. To disable use of the Domain Name System (DNS), use the **no** form of this command.

**ip domain name** *name*

**no ip domain name** *name*

<b>Syntax Description</b>	<i>name</i>	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name.
---------------------------	-------------	---

<b>Defaults</b>	Enabled
-----------------	---------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
	12.2	The syntax of the command changed from <b>ip domain-name</b> to <b>ip domain name</b> .

**Usage Guidelines** Any IP host name that does not contain a domain name (that is, any name without a dot) will have the dot and cisco.com appended to it before being added to the host table.

The Cisco IOS software will still accept the previous version of the command, which is **ip domain-name**.

**Examples** The following example defines cisco.com as the default domain name:

```
ip domain name cisco.com
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip domain list</b>	Defines a list of default domain names to complete unqualified host names.
	<b>ip domain lookup</b>	Enables the IP DNS-based host name-to-address translation.
	<b>ip domain retry</b>	Specifies the number of times to retry sending DNS queries.
	<b>ip domain timeout</b>	Specifies the amount of time to wait for a response to a DNS query.
	<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.



# ip domain retry

To specify the number of times to retry sending Domain Name System (DNS) queries, use the **ip domain retry** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

**ip domain retry** *number*

**no ip domain retry** *number*

<b>Syntax Description</b>	<i>number</i>	Number of times to retry sending a DNS query to the DNS server. The range is from 0 to 100; the default is 2.
---------------------------	---------------	---

<b>Defaults</b>	<i>number</i> : 2 times
-----------------	-------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3	This command was introduced.

<b>Usage Guidelines</b>	If the <b>ip domain retry</b> command is not configured, the Cisco IOS software will only send DNS queries out twice.
-------------------------	---

<b>Examples</b>	The following example shows how to configure the router to send out 10 DNS queries before giving up: <pre>ip domain retry 10</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip domain list</b>	Defines a list of default domain names to complete unqualified host names.
	<b>ip domain lookup</b>	Enables the IP DNS-based host name-to-address translation.
	<b>ip domain retry</b>	Specifies the number of times to retry sending DNS queries.
	<b>ip domain timeout</b>	Specifies the amount of time to wait for a response to a DNS query.
	<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.

# ip domain round-robin

To enable round-robin functionality on DNS servers, use the **ip domain round-robin** command in global configuration mode. To disable round-robin functionality, use the no form of the command.

**ip domain round-robin**

**no ip domain round-robin**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Round robin is not enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.

**Usage Guidelines**

In a multiple server configuration *without* the DNS round-robin functionality, the first host server/IP address is used for the whole time to live (TTL) of the cache, and uses the second and third only in the event of host failure. This behavior presents a problem when a high volume of users all arrive at the first host during the TTL time. The network access server (NAS) then sends out a DNS query; the DNS servers reply with a list of the configured IP addresses to the NAS. The NAS then caches these IP addresses for a given time (for example, five minutes). All users that dial in during the five minute TTL time will land on one host, the first IP address in the list.

In a multiple server configuration *with* the DNS round-robin functionality, the DNS server returns the IP address of all hosts to rotate between the cache of host names. During the TTL of the cache, users are distributed among the hosts. This functionality distributes calls across the configured hosts and reduces the amount of DNS queries.

**Examples**

The following example allows a Telnet to www.company.com to connect to each of the three IP addresses specified in the following order: the first time the Telnet command is given, it would connect to 10.0.0.1; the second time the command is given, it would connect to 20.0.0.1; and the third time the command is given, it would connect to 30.0.0.1. In each case, the other two addresses would also be tried if the first one failed; this is the normal operation of the Telnet command.

```
Router(config)# ip host www.company.com 10.0.0.1 20.0.0.1 30.0.0.1
Router(config)# ip domain round-robin
```

# ip domain timeout

To specify the amount of time to wait for a response to a DNS query, use the **ip domain timeout** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

**ip domain timeout** *seconds*

**no ip domain timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Time, in seconds, to wait for a response to a DNS query. The range is from 0 to 3600; the default is 3.												
<b>Defaults</b>	<i>seconds</i> : 3 seconds													
<b>Command Modes</b>	Global configuration													
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.3	This command was introduced.									
Release	Modification													
12.3	This command was introduced.													
<b>Usage Guidelines</b>	If the <b>ip domain timeout</b> command is not configured, the Cisco IOS software will only wait 3 seconds for a response to a DNS query.													
<b>Examples</b>	<p>The following example shows how to configure the router to wait 50 seconds for a response to a DNS query:</p> <pre>ip domain timeout 50</pre>													
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>ip domain list</b></td> <td>Defines a list of default domain names to complete unqualified host names.</td> </tr> <tr> <td><b>ip domain lookup</b></td> <td>Enables the IP DNS-based host name-to-address translation.</td> </tr> <tr> <td><b>ip domain retry</b></td> <td>Specifies the number of times to retry sending DNS queries.</td> </tr> <tr> <td><b>ip domain timeout</b></td> <td>Specifies the amount of time to wait for a response to a DNS query.</td> </tr> <tr> <td><b>ip name-server</b></td> <td>Specifies the address of one or more name servers to use for name and address resolution.</td> </tr> </tbody> </table>	Command	Description	<b>ip domain list</b>	Defines a list of default domain names to complete unqualified host names.	<b>ip domain lookup</b>	Enables the IP DNS-based host name-to-address translation.	<b>ip domain retry</b>	Specifies the number of times to retry sending DNS queries.	<b>ip domain timeout</b>	Specifies the amount of time to wait for a response to a DNS query.	<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.	
Command	Description													
<b>ip domain list</b>	Defines a list of default domain names to complete unqualified host names.													
<b>ip domain lookup</b>	Enables the IP DNS-based host name-to-address translation.													
<b>ip domain retry</b>	Specifies the number of times to retry sending DNS queries.													
<b>ip domain timeout</b>	Specifies the amount of time to wait for a response to a DNS query.													
<b>ip name-server</b>	Specifies the address of one or more name servers to use for name and address resolution.													

# ip drp access-group

To control the sources of Director Response Protocol (DRP) queries to the DRP Server Agent, use the **ip drp access-group** command in global configuration mode. To remove the access list, use the **no** form of this command.

**ip drp access-group** *access-list-number*

**no ip drp access-group** *access-list-number*

<b>Syntax Description</b>	<i>access-list-number</i>	Number of a standard IP access list in the range from 1 to 99 or from 1300 to 1999.
---------------------------	---------------------------	---

**Defaults** The DRP Server Agent will answer all queries.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.2 F	This command was introduced.

**Usage Guidelines** This command applies an access list to the interface, thereby controlling which devices can send queries to the DRP Server Agent.

If both an authentication key chain and an access group have been specified, both security measures must permit access before a request is processed.

**Examples** The following example configures access list 1, which permits only queries from the host at 33.45.12.4:

```
access-list 1 permit 33.45.12.4
ip drp access-group 1
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip drp authentication key-chain</b>	Configures authentication on the DRP Server Agent for DistributedDirector.
	<b>show ip drp</b>	Displays information about the DRP Server Agent for DistributedDirector.

# ip drp authentication key-chain

To configure authentication on the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **ip drp authentication key-chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

**ip drp authentication key-chain** *name-of-chain*

**no ip drp authentication key-chain** *name-of-chain*

## Syntax Description

*name-of-chain* Name of the key chain containing one or more authentication keys.

## Defaults

No authentication is configured for the DRP Server Agent.

## Command Modes

Global configuration

## Command History

Release	Modification
11.2 F	This command was introduced.

## Usage Guidelines

When a key chain and key are configured, the key is used to authenticate all DRP requests and responses. The active key on the DRP Server Agent must match the active key on the primary agent. Use the **key** and **key-string** commands to configure the key.

## Examples

The following example configures a key chain named *ddchain*:

```
ip drp authentication key-chain ddchain
```

## Related Commands

Command	Description
<b>accept-lifetime</b>	Sets the time period during which the authentication key on a key chain is received as valid.
<b>ip drp access-group</b>	Controls the sources of DRP queries to the DRP Server Agent.
<b>key</b>	Identifies an authentication key on a key chain.
<b>key chain</b>	Enables authentication for routing protocols.
<b>key-string (authentication)</b>	Specifies the authentication string for a key.
<b>send-lifetime</b>	Sets the time period during which an authentication key on a key chain is valid to be sent.
<b>show ip drp</b>	Displays information about the DRP Server Agent for DistributedDirector.
<b>show key chain</b>	Displays authentication key information.

# ip drp server

To enable the Director Response Protocol (DRP) Server Agent that works with DistributedDirector, use the **ip drp server** command in global configuration mode. To disable the DRP Server Agent, use the **no** form of this command.

**ip drp server**

**no ip drp server**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	11.2 F	This command was introduced.

**Examples** The following example enables the DRP Server Agent:

```
ip drp server
```

Related Commands	Command	Description
	<b>ip drp access-group</b>	Controls the sources of DRP queries to the DRP Server Agent.
	<b>ip drp authentication key-chain</b>	Configures authentication on the DRP Server Agent for DistributedDirector.
	<b>show ip drp</b>	Displays information about the DRP Server Agent for DistributedDirector.

# ip forward-protocol

To specify which protocols and ports the router forwards when forwarding broadcast packets, use the **ip forward-protocol** command in global configuration mode. To remove a protocol or port, use the **no** form of this command.

```
ip forward-protocol { udp [port] | nd | sdns }
```

```
no ip forward-protocol { udp [port] | nd | sdns }
```

Syntax Description	Field	Description
	<b>udp</b>	Forwards User Datagram Protocol (UDP) datagrams. See the “Defaults” section for a list of port numbers forwarded by default.
	<i>port</i>	(Optional) Destination port that controls which UDP services are forwarded.
	<b>nd</b>	Forwards Network Disk (ND) datagrams. This protocol is used by older diskless Sun workstations.
	<b>sdns</b>	Secure Data Network Service.

Defaults	Enabled
----------	---------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines**

Enabling a helper address or UDP flooding on an interface causes the Cisco IOS software to forward particular broadcast packets. You can use the **ip forward-protocol** command to specify exactly which types of broadcast packets you would like to have forwarded. A number of commonly forwarded applications are enabled by default. Enabling forwarding for some ports (for example, Routing Information Protocol (RIP)) may be hazardous to your network.

If you use the **ip forward-protocol** command, specifying only UDP without the port enables forwarding and flooding on the default ports.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP). DHCP is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the software. The DHCP server now receives broadcasts from the DHCP clients.

If an IP helper address is defined, UDP forwarding is enabled on default ports. If UDP flooding is configured, UDP flooding is enabled on the default ports.

If a helper address is specified and UDP forwarding is enabled, broadcast packets destined to the following port numbers are forwarded by default:

- Trivial File Transfer Protocol (TFTP) (port 69)
- Domain Naming System (port 53)
- Time service (port 37)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- Boot Protocol (BOOTP) client and server datagrams (ports 67 and 68)
- TACACS service (port 49)
- IEN-116 Name Service (port 42)



# ip forward-protocol spanning-tree

To permit IP broadcasts to be flooded throughout the internetwork in a controlled fashion, use the **ip forward-protocol spanning-tree** command in global configuration mode. To disable the flooding of IP broadcasts, use the **no** form of this command.

**ip forward-protocol spanning-tree [any-local-broadcast]**

**no ip forward-protocol spanning-tree [any-local-broadcast]**

<b>Syntax Description</b>	<b>any-local-broadcast</b> (Optional) Accept any local broadcast when flooding.				
<b>Defaults</b>	Disabled				
<b>Command Modes</b>	Global configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.
Release	Modification				
10.0	This command was introduced.				

**Usage Guidelines**

A packet must meet the following criteria to be considered for flooding:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).
- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface; major-net broadcast for the receiving interface if the **ip classless** command is also configured; or any local IP broadcast address if the **ip forward-protocol spanning-tree any-local-broadcast** command is configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, or BOOTP packet, or a UDP port specified by the **ip forward-protocol udp** global configuration command.

A flooded UDP datagram is given the destination address specified by the **ip broadcast-address** interface configuration command on the output interface. The destination address can be set to any desired address. Thus, the destination address may change as the datagram propagates through the network. The source address is never changed. The TTL value is decremented.

After a decision has been made to send the datagram out on an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines and is therefore subject to access lists, if they are present on the output interface.

The **ip forward-protocol spanning-tree** command uses the database created by the bridging Spanning-Tree Protocol. Therefore, the transparent bridging option must be in the routing software, and bridging must be configured on each interface that is to participate in the flooding in order to support this capability.

If an interface does not have bridging configured, it still will be able to receive broadcasts, but it will never forward broadcasts received on that interface. Also, it will never use that interface to send broadcasts received on a different interface.

If no actual bridging is desired, you can configure a type-code bridging filter that will deny all packet types from being bridged. Refer to the “Configuring Transparent Bridging” chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more information about using access lists to filter bridged traffic. The spanning-tree database is still available to the IP forwarding code to use for the flooding.

The spanning-tree-based flooding mechanism forwards packets whose contents are all ones (255.255.255.255), all zeros (0.0.0.0), and, if subnetting is enabled, all networks (131.108.255.255 as an example in the network number 131.108.0.0). This mechanism also forward packets whose contents are the zeros version of the all-networks broadcast when subnetting is enabled (for example, 131.108.0.0).

This command is an extension of the **ip helper-address** interface configuration command, in that the same packets that may be subject to the helper address and forwarded to a single network can now be flooded. Only one copy of the packet will be put on each network segment.

### Examples

The following example permits IP broadcasts to be flooded through the internetwork in a controlled fashion:

```
ip forward-protocol spanning-tree
```

### Related Commands

Command	Description
<b>ip broadcast-address</b>	Defines a broadcast address for an interface.
<b>ip forward-protocol</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
<b>ip forward-protocol turbo-flood</b>	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
<b>ip helper-address</b>	Forwards UDP broadcasts, including BOOTP, received on an interface.

# ip forward-protocol turbo-flood

To speed up flooding of User Datagram Protocol (UDP) datagrams using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** command in global configuration mode. To disable this feature, use the **no** form of this command.

**ip forward-protocol turbo-flood**

**no ip forward-protocol turbo-flood**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Release	Modification
10.0	This command was introduced.

---

---

**Usage Guidelines** Used in conjunction with the **ip forward-protocol spanning-tree** global configuration command, this feature is supported over Advanced Research Projects Agency (ARPA)-encapsulated Ethernets, FDDI, and High-Level Data Link Control (HDLC) encapsulated serials, but is not supported on Token Rings. As long as the Token Rings and the non-HDLC serials are not part of the bridge group being used for UDP flooding, turbo flooding will behave normally.

---

**Examples** The following is an example of a two-port router using this command:

```
ip forward-protocol turbo-flood
ip forward-protocol spanning-tree
!
interface ethernet 0
 ip address 128.9.1.1
 bridge-group 1
!
interface ethernet 1
 ip address 128.9.1.2
 bridge-group 1
!
bridge 1 protocol dec
```

Related Commands	Command	Description
	<b>ip forward-protocol</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
	<b>ip forward-protocol spanning-tree</b>	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

# ip helper-address

To enable the forwarding of User Datagram Protocol (UDP) broadcasts, including BOOTP, received on an interface, use the **ip helper-address** command in interface configuration mode. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

```
ip helper-address [vrf name | global] address [redundancy vrg-name]
```

```
no ip helper-address [vrf name | global] address [redundancy vrg-name]
```

Syntax Description		
<b>vrf name</b>	(Optional) Enables VPN routing and forwarding (VRF) instance and VRF name.	
<b>global</b>	(Optional) Configures a global routing table.	
<i>address</i>	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.	
<b>redundancy</b> <i>vrg-name</i>	(Optional) Defines the VRG group name.	

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(4)B	The <b>vrf name</b> keyword and argument combination was added, and the <b>global</b> keyword was added.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(15)T	The <b>redundancy vrg-name</b> keyword and argument combination was added.

**Usage Guidelines** Combined with the **ip forward-protocol** global configuration command, the **ip helper-address** command allows you to control which broadcast packets and which protocols are forwarded.

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. To enable BOOTP or DHCP broadcast forwarding for a set of clients, configure a helper address on the router interface connected to the client. The helper address should specify the address of the BOOTP or DHCP server. If you have multiple servers, you can configure one helper address for each server.

All of the following conditions must be met in order for a UDP or IP packet to be helpered by the **ip helper-address** command:

- The MAC address of the received frame must be all-ones broadcast address (ffff.ffff.ffff).

- The IP destination address must be one of the following: all-ones broadcast (255.255.255.255), subnet broadcast for the receiving interface, or major-net broadcast for the receiving interface if the **no ip classless** command is also configured.
- The IP time-to-live (TTL) value must be at least 2.
- The IP protocol must be UDP (17).
- The UDP destination port must be for TFTP, Domain Name System (DNS), Time, NetBIOS, ND, BOOTP or DHCP packet, or a UDP port specified by the **ip forward-protocol udp** global configuration command.

If the DHCP server resides in a Virtual Private Network (VPN) or global space that is different from the interface VPN, then the **vrf name** or **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-address vrf name address** option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-address vrf name address** command is configured and later the **vrf** is deleted from the configuration, then all IP helper addresses associated with that VRF name will be removed from the interface configuration.

If the **ip helper-address address** command is already configured on an interface with no VRF name configured, and later the interface is configured with the **ip helper-address vrf name address** command, then the previously configured **ip helper-address address** is considered to be global.



#### Note

The **ip helper-address** command does not work on an X.25 interface on a destination router because the router cannot determine if the packet was intended as a physical broadcast.

#### Examples

The following example defines an address that acts as a helper address:

```
interface ethernet 1
 ip helper-address 121.24.43.2
```

The following example defines an address that acts as a helper address and is associated with the VRF named red:

```
interface ethernet 1/0
 ip helper-address vrf red 121.25.44.2
```

The following example defines an address that acts as a helper address and is associated with the VRG named shop:

```
interface ethernet 1/0
 ip helper-address 121.25.45.2 redundancy shop
```

#### Related Commands

Command	Description
<b>ip forward-protocol</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

# ip host

To define a static host name-to-address mapping in the host cache, use the **ip host** command in global configuration mode. To remove the host name-to-address mapping, use the **no** form of this command.

```
ip host {name / tmodem-telephone-number} [tcp-port-number] {address1 [address2...address8]}
```

```
no ip host {name / tmodem-telephone-number} address1
```

Syntax Description	
<i>name</i>	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform are limited.
<i>tmodem-telephone-number</i>	Modem telephone number that is mapped to the IP host address for use in Cisco modem user interface mode (you must enter the letter “t” before the telephone number).
<i>tcp-port-number</i>	(Optional) TCP port number to connect to when using the defined host name in conjunction with an EXEC connect or Telnet command. The default is Telnet (port 23).
<i>address1</i>	Associated IP host address.
<i>address2...address8</i>	(Optional) Additional associated IP addresses. You can bind up to eight addresses to a host name.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(4)T	The capability to map a modem telephone number to an IP host was added for the Cisco modem user interface feature.

**Usage Guidelines** The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as **ping**) are limited.

**Examples** The following example defines two static mappings:

```
ip host croff 192.168.7.18
ip host bisso-gw 10.2.0.2 192.168.7.33
```

The following example shows how to map modem telephone number (415) 555-1234 to IP host address 10.1.5.5 for the Cisco modem user interface mode:

```
ip host t4155551234 10.1.5.5
```

## ip icmp rate-limit unreachable

To have the Cisco IOS software limit the rate at which Internet Control Message Protocol (ICMP) destination unreachable messages are generated, use the **ip icmp rate-limit unreachable** command in global configuration mode. To remove the rate limit, use the **no** form of this command.

**ip icmp rate-limit unreachable** [**df**] *milliseconds*

**no ip icmp rate-limit unreachable** [**df**]

Syntax Description	<b>df</b>	(Optional) Limits the rate ICMP destination unreachable messages are sent when code 4, fragmentation is needed and DF set, is specified in the IP header of the ICMP destination unreachable message.
	<i>milliseconds</i>	Time limit (in milliseconds) in which one ICMP destination unreachable message is sent. The range is 1 millisecond to 4294967295 milliseconds.

**Defaults** The default value is one ICMP destination unreachable message per 500 milliseconds.

**Command Modes** Global configuration

Command History	Release	Modification
	12.0	This command was introduced.

**Usage Guidelines** The **no ip icmp rate-limit unreachable** command turns off the previously configured rate limit. To re-set the rate limit to its default value, use the **default ip icmp rate-limit unreachable** command.

The Cisco IOS software maintains two timers: one for general destination unreachable messages and one for DF destination unreachable messages. Both share the same time limits and defaults. If the **df** option is not configured, the **ip icmp rate-limit unreachable** command sets the time values for DF destination unreachable messages. If the **df** option is configured, its time values remain independent from those of general destination unreachable messages.

**Examples** The following example sets the rate of the ICMP destination unreachable message to one message every 10 milliseconds:

```
ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
no ip icmp rate-limit unreachable
```

The following example sets the rate limit back to the default:

```
default ip icmp rate-limit unreachable
```



# ip icmp redirect

To control the type of Internet Control Message Protocol (ICMP) redirect message that is sent by the Cisco IOS software, use the **ip icmp redirect** command in global configuration mode. To set the value back to the default, use the **no** form of this command.

**ip icmp redirect** [host | subnet]

**no ip icmp redirect** [host | subnet]

## Syntax Description

<b>host</b>	(Optional) Sends ICMP host redirects.
<b>subnet</b>	(Optional) Sends ICMP subnet redirects.

## Defaults

The router will send ICMP subnet redirect messages.

Because the **ip icmp redirect subnet** command is the default, the command will not be displayed in the configuration.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0	This command was introduced.

## Usage Guidelines

An ICMP redirect message can be generated by a router when a packet is received and transmitted on the same interface. In this situation, the router will forward the original packet and send a ICMP redirect message back to the sender of the original packet. This behavior allows the sender to bypass the router and forward future packets directly to the destination (or a router closer to the destination).

There are two types of ICMP redirect messages: redirect for a host address or redirect for an entire subnet.

The **ip icmp redirect** command determines the type of ICMP redirects sent by the system and is configured on a per system basis. Some hosts do not understand ICMP subnet redirects and need the router to send out ICMP host redirects. Use the **ip icmp redirect host** command to have the router send out ICMP host redirects. Use the **ip icmp redirect subnet** command to set the value back to the default, which is to send subnet redirects.

To prevent the router from sending ICMP redirects, use the **no ip redirects** interface configuration command.

## Examples

The following example enables the router to send out ICMP host redirects:

```
ip icmp redirect hosts
```

The following example sets the value back to the default, which is subnet redirects:

```
ip icmp redirect subnet
```

■ ip icmp redirect

---

**Related Commands**

Command	Description
<b>ip redirects</b>	Enables the sending of ICMP redirect messages.

---

# ip information-reply

To have the Cisco IOS software send Internet Control Message Protocol (ICMP) information replies, use the **ip information-reply** command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip information-reply**

**no information-reply**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Release	Modification
12.2T	This command was introduced.

---

---

**Usage Guidelines** The ability for the Cisco IOS software to respond to ICMP information request messages with an ICMP information reply message is disabled by default. Use this command to allow the software to send ICMP information reply messages.

---

**Examples** The following example enables the sending of ICMP information reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 131.108.1.0 255.255.255.0
 ip information-reply
```

# ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** interface configuration command. To disable IRDP routing, use the **no** form of this command.

**ip irdp** [**multicast** | **holdtime** *seconds* | **maxadvertinterval** *seconds* | **minadvertinterval** *seconds* | **preference** *number* | **address** *address* [*number*]]

**no ip irdp**

Syntax Description	
<b>multicast</b>	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.
<b>holdtime</b> <i>seconds</i>	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the <b>maxadvertinterval</b> value. Must be greater than <b>maxadvertinterval</b> and cannot be greater than 9000 seconds.
<b>maxadvertinterval</b> <i>seconds</i>	(Optional) Maximum interval in seconds between advertisements. The range is from 1 to 1800. A value of 0 means only advertise when solicited. The default is 600 seconds.
<b>minadvertinterval</b> <i>seconds</i>	(Optional) Minimum interval in seconds between advertisements. The range is from 1 to 1800. The default is 450 seconds.
<b>preference</b> <i>number</i>	(Optional) Preference value. The allowed range is $-2^{31}$ to $2^{31}$ . The default is 0. A higher value increases the preference level of the router. You can modify a particular router so that it will be the preferred router to which other routers will home.
<b>address</b> <i>address</i> [ <i>number</i> ]	(Optional) IP address ( <i>address</i> ) to proxy advertise, and optionally, its preference value ( <i>number</i> ).

## Defaults

Disabled

When enabled, IRDP uses these defaults:

- Broadcast IRDP advertisements
- Maximum interval between advertisements: 600 seconds
- Minimum interval between advertisements: 450 seconds
- Preference: 0

## Command Modes

Interface configuration

## Command History

Release	Modification
10.0	This command was introduced.

**Usage Guidelines**

If you change the **maxadvertinterval** value, the other two values also change, so it is important to change the **maxadvertinterval** value before changing either the **holdtime** or **minadvertinterval** values.

The **ip irdp multicast** command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.

**Examples**

The following example sets the various IRDP processes:

```
! enable irdp on interface Ethernet 0
interface ethernet 0
 ip irdp
! send IRDP advertisements to the multicast address
 ip irdp multicast
! increase router preference from 100 to 50
 ip irdp preference 50
! set maximum time between advertisements to 400 secs
 ip irdp maxadvertinterval 400
! set minimum time between advertisements to 100 secs
 ip irdp minadvertinterval 100
! advertisements are good for 6000 seconds
 ip irdp holdtime 6000
! proxy-advertise 131.108.14.5 with default router preference
 ip irdp address 131.108.14.5
! proxy-advertise 131.108.14.6 with preference of 50
 ip irdp address 131.108.14.6 50
```

**Related Commands**

Command	Description
<b>show ip irdp</b>	Displays IRDP values.

# ip local-proxy-arp

To enable the local proxy Address Resolution Protocol (ARP) feature, use the **ip local-proxy-arp** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**ip local-proxy-arp**

**no ip local-proxy-arp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command is not enabled by default.

**Command Modes** Interface configuration

## Command History

Release	Modification
12.1(5c)EX	This command was introduced on the Catalyst 6500 series switches.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E on the Catalyst 6500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

## Usage Guidelines

The local proxy ARP feature allows the Multilayer Switching Feature Card (MSFC) to respond to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, the MSFC responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly to the Catalyst 6500 series switch on which they are connected.

Before the local proxy ARP feature can be used, the IP proxy ARP feature must be enabled. The IP proxy ARP feature is enabled by default.

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces where the local proxy ARP feature is enabled.

## Examples

The following example shows how to enable the local proxy ARP feature:

```
Router(config-if)# ip local-proxy-arp
```

# ip mask-reply

To have the Cisco IOS software respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP mask reply messages, use the **ip mask-reply** command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip mask-reply**

**no ip mask-reply**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Interface configuration

---

Command History	Release	Modification
	10.0	This command was introduced.

---



---

**Examples** The following example enables the sending of ICMP mask reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 131.108.1.0 255.255.255.0
 ip mask-reply
```

# ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

**ip mobile arp** [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

**no ip mobile arp** [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

Syntax Description		
<b>timers</b>	(Optional) Indicates that you are setting local-area mobility timers.	
<i>keepalive</i>	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 5 minutes (300 seconds).	
<i>hold-time</i>	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default hold time is 15 minutes (900 seconds).	
<b>access-group</b>	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.	
<i>access-list-number</i>	(Optional) Number of a standard IP access list. It is a decimal number from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.	
<i>name</i>	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.	

## Defaults

Local-area mobility is disabled.

If you enable local-area mobility:

*keepalive*: 5 minutes (300 seconds)

*hold-time*: 15 minutes (900 seconds)

## Command Modes

Interface configuration

## Command History

Release	Modification
11.0	This command was introduced.

## Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.



To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be taken for mobile nodes and disrupt normal operations.

### Examples

The following example configures local-area mobility on Ethernet interface 0:

```
access-list 10 permit 198.92.37.114
 interface ethernet 0
 ip mobile arp access-group 10
```

### Related Commands

Command	Description
<b>access-list (IP standard)</b>	Defines a standard IP access list.
<b>default-metric (BGP)</b>	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
<b>default-metric (OSPF)</b>	Sets default metric values for OSPF.
<b>default-metric (RIP)</b>	Sets default metric values for RIP.
<b>network (BGP)</b>	Specifies the list of networks for the BGP routing process.
<b>network (IGRP)</b>	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
<b>network (RIP)</b>	Specifies a list of networks for the RIP routing process.
<b>redistribute (IP)</b>	Redistributes routes from one routing domain into another routing domain.
<b>router eigrp</b>	Configures the IP Enhanced IGRP routing process.
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
<b>router ospf</b>	Configures an OSPF routing process.

# ip mtu

To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

**ip mtu** *bytes*

**no ip mtu**

<b>Syntax Description</b>	<i>bytes</i>	MTU in bytes.
---------------------------	--------------	---------------

<b>Defaults</b>	Minimum is 128 bytes; maximum depends on the interface medium.
-----------------	--

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	If an IP packet exceeds the MTU set for the interface, the Cisco IOS software will fragment it. All devices on a physical medium must have the same protocol MTU in order to operate.
-------------------------	---



**Note**

Changing the MTU value (with the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value, and you change the MTU value, the IP MTU value will be modified automatically to match the new MTU. However, the reverse is not true; changing the IP MTU value has no effect on the value for the **mtu** command.

<b>Examples</b>	The following example sets the maximum IP packet size for the first serial interface to 300 bytes:
-----------------	--

```
interface serial 0
 ip mtu 300
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>mtu</b>	Adjusts the maximum packet size or MTU size.

# ip name-server

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** command in global configuration mode. To remove the addresses specified, use the **no** form of this command.

**ip name-server** *server-address1* [*server-address2...server-address6*]

**no ip name-server** *server-address1* [*server-address2...server-address6*]

Syntax Description	
<i>server-address1</i>	IPv4 or IPv6 addresses of a name server.
<i>server-address2...server-address6</i>	(Optional) IP addresses of additional name servers (a maximum of six name servers).

**Defaults** No name server addresses are specified.

**Command Modes** Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S	Support for IPv6 addresses was added.

**Examples** The following example specifies IPv4 hosts 172.16.1.111 and 172.16.1.2 as the name servers:

```
ip name-server 172.16.1.111 172.16.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 172.16.1.111
ip name-server 172.16.1.2
```

The following example specifies IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

This command will be reflected in the configuration file as follows:

```
ip name-server 3FFE:C00::250:8BFF:FEE8:F800
ip name-server 2001:0DB8::3
```

Related Commands	Command	Description
	<b>ip domain-lookup</b>	Enables the IP DNS-based host name-to-address translation.
	<b>ip domain-name</b>	Defines a default domain name to complete unqualified host names (names without a dotted decimal domain name).

# ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), to enable NAT logging, or to enable static IP address support, use the **ip nat** command in interface configuration mode. To prevent the interface from being able to translate or log, use the **no** form of this command.

```
ip nat [{inside | outside}] | log | translations | syslog | allow-static-host]
```

```
no ip nat [{inside | outside}] | log | translations | syslog | allow-static-host]
```

## Syntax Description

<b>inside</b>	(Optional) Indicates that the interface is connected to the inside network (the network subject to NAT translation).
<b>outside</b>	(Optional) Indicates that the interface is connected to the outside network.
<b>log</b>	(Optional) Enables NAT logging.
<b>translations</b>	(Optional) Enables NAT logging translations.
<b>syslog</b>	(Optional) Enables syslog for NAT logging translations.
<b>allow-static-host</b>	(Optional) Enables static IP address support for NAT translation.

## Defaults

Traffic leaving or arriving at this interface is not subject to NAT.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The <b>allow-static-host</b> keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.

## Usage Guidelines

Only packets moving between inside and outside interfaces can be translated. You must specify at least one inside interface and outside interface for each border router where you intend to use NAT.

When static IP address support is enabled with the **ip nat allow-static-host** command, Cisco IOS software will provide a working IP address within the Public Wireless LAN to users configured with a static IP address.

## Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
```

```

ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

```

The following example enables static IP address support for the router at 192.168.196.51:

```

interface ethernet 1
 ip nat inside
 ip nat allow-static-host
 ip nat pool xyz 171.1.1.1 171.1.1.10 netmask 255.255.255.0 accounting WLAN-ACCT
 ip nat inside source list 1 pool net-208
 access-list 1 deny ip 192.168.196.51

```

#### Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>debug ip nat</b>	Displays information about IP packets translated by NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat inside destination

To enable Network Address Translation (NAT) of the inside destination address, use the **ip nat inside destination** command in global configuration mode. To remove the dynamic association to a pool, use the **no** form of this command.

**ip nat inside destination list** {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]

**no ip nat inside destination list** {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]

## Syntax Description

<b>list</b> <i>access-list-number</i>	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
<b>list</b> <i>name</i>	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
<b>pool</b> <i>name</i>	Name of the pool from which global IP addresses are allocated during dynamic translation.
<b>mapping-id</b> <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

## Defaults

No inside destination addresses are translated.

## Command Modes

Global configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.3(7)T	The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added.

## Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

## Examples

The following example shows how to translate between inside hosts addressed to either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside destination list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
```

## ip nat inside destination

```

interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
Need example for mapping-id

```

## Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

## Dynamic NAT

**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **vrf** *name*]

**no ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **vrf** *name*]

## Static NAT

**ip nat inside source** {**static** {**esp** *local-ip* **interface** *type number* | *local-ip* *global-ip*}} [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

**no ip nat inside source** {**static** {**esp** *local-ip* **interface** *type number* | *local-ip* *global-ip*}} [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

## Port Static NAT

**ip nat inside source** {**static** {**tcp** | **udp** {*local-ip* *local-port* *global-ip* *global-port* | **interface** *global-port*}}} [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

**no ip nat inside source** {**static** {**tcp** | **udp** {*local-ip* *local-port* *global-ip* *global-port* | **interface** *global-port*}}} [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

## Network Static NAT

**ip nat inside source static network** *local-network* *global-network* *mask* [**extendable** | **no-alias** | **no-payload** | **mapping-id** *map-id* | **redundancy** *group-name* | **route-map** | **vrf** *name*]

**no ip nat inside source static network** *local-network* *global-network* *mask* [**extendable** | **no-alias** | **no-payload** | **mapping-id** *map-id* | **redundancy** *group-name* | **route-map** | **vrf** *name*]

## Syntax Description

<b>list</b> <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
<b>list</b> <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
<b>route-map</b> <i>name</i>	Specifies the named route map.
<b>interface</b> <i>type</i>	Specifies the interface type for the global address.
<b>interface</b> <i>number</i>	Specifies the interface number for the global address.



<b>pool</b> <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
<b>mapping-id</b> <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
<b>vrf</b> <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
<b>overload</b>	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
<b>static</b> <i>local-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
<i>local-port</i>	Sets the local TCP/UDP port in a range from 1 to 65535.
<b>static</b> <i>global-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the globally unique IP address of an inside host as it appears to the outside network.
<i>global-port</i>	Sets the global TCP/UDP port in a range from 1 to 65535.
<b>extendable</b>	(Optional) Extends the translation.
<b>no-alias</b>	(Optional) Prohibits an alias from being created for the global address.
<b>no-payload</b>	(Optional) Prohibits the translation of an embedded address or port in the payload.
<b>redundancy</b> <i>group-name</i>	(Optional) Establishes NAT redundancy.
<b>esp</b> <i>local-ip</i>	Establishes IPSec-ESP (tunnel mode) support.
<b>tcp</b>	Establishes the Transmission Control Protocol.
<b>udp</b>	Establishes the User Datagram Protocol.
<b>network</b> <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	Specifies the global subnet translation.
<i>mask</i>	Established the IP Network mask to be with used with subnet translations.

**Defaults**

No NAT translation of inside source addresses occurs.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the <b>route-map</b> <i>name</i> keyword and argument combination was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the <b>redundancy</b> <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the <b>no-payload</b> keyword was added.
12.2(13)T	The <b>interface</b> keyword was added for static translations. The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added for dynamic translations. The <b>vrf</b> <i>name</i> keyword and argument combination was added.
12.3(7)T	The static <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added.

**Usage Guidelines**

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the keyword **static** establishes a single static translation.

**Examples**

The following example shows how to translate between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example shows how to translate only traffic local to the providers edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface e 0 vrf shop overload
ip nat inside source list 1 interface e 0 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 192.1.1.1
ip route vrf bank 0.0.0.0 0.0.0.0 192.1.1.1
!
access-list 1 permit 10.1.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface e 1 vrf shop overload
ip nat inside source list 1 interface e 1 vrf bank overload
```

## ip nat inside source

```

!
ip route vrf shop 0.0.0.0 0.0.0.0 172.1.1.1 global
ip route vrf bank 0.0.0.0 0.0.0.0 172.1.1.1 global
access-list 1 permit 10.1.1.0 0.0.0.255

```

## Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

## Dynamic NAT

```
ip nat outside source {list {access-list-number | access-list-name} | route-map name} pool
pool-name [add-route | mapping-id map-id | vrf name]
```

```
no ip nat outside source {list {access-list-number | access-list-name} | route-map name} pool
pool-name [add-route | mapping-id map-id | vrf name]
```

## Static NAT

```
ip nat outside source static global-ip local-ip [add-route | extendable | mapping-id map-id |
no-alias | no-payload | redundancy group-name | vrf name]
```

```
no ip nat outside source static global-ip local-ip [add-route | extendable | mapping-id map-id |
no-alias | no-payload | redundancy group-name | vrf name]
```

## Port Static NAT

```
ip nat outside source static {tcp | udp} global-ip global-port local-ip local-port [add-route |
extendable | mapping-id map-id | no-alias | no-payload | redundancy group-name | vrf name]
```

```
no ip nat outside source static {tcp | udp} global-ip global-port local-ip local-port [add-route |
extendable | mapping-id map-id | no-alias | no-payload | redundancy group-name | vrf name]
```

## Network Static NAT

```
ip nat outside source static network global-network local-network mask [add-route | extendable
| mapping-id map-id | no-alias | no-payload | redundancy | vrf name]
```

```
no ip nat outside source static network global-network local-network mask [add-route |
extendable | mapping-id map-id | no-alias | no-payload | redundancy | vrf name]
```

## Syntax Description

<b>list</b> <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
<b>list</b> <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
<b>route-map</b> <i>name</i>	Specifies a named route map.
<b>pool</b> <i>pool-name</i>	Name of the pool from which global IP addresses are allocated.
<b>mapping-id</b> <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
<b>vrf</b> <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN.
<b>add-route</b>	(Optional) Adds a static route for the outside local address.

<b>static</b> <i>global-ip</i>	Sets up a single static translation. This argument establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.
<i>local-ip</i>	Local IP address of an outside host as it appears to the inside network. The address was allocated from address space routable on the inside (RFC 1918, <i>Address Allocation for Private Internets</i> ).
<b>extendable</b>	(Optional) Extends the transmission.
<b>no-alias</b>	(Optional) Prohibits an alias from being created for the local address.
<b>no-payload</b>	(Optional) Prohibits the translation of embedded address or port in the payload.
<b>redundancy</b> <i>group-name</i>	(Optional) Enables the NAT redundancy operation.
<b>tcp</b>	Establishes the Transmission Control Protocol.
<b>udp</b>	Establishes the User Datagram Protocol.

**Defaults**

No translation of source addresses coming from the outside to the inside network occurs.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the <b>redundancy</b> <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the <b>no-payload</b> keyword was added.
12.2(13)T	The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added for dynamic translations. The <b>vrf</b> <i>name</i> keyword and argument combination was added.
12.3(7)T	The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added for static translations.

**Usage Guidelines**

You might have IP addresses that are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this command if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or routers.

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

The following example shows how to translate between inside hosts addressed from the 9.114.11.0 network to the globally unique 171.69.233.208/28 network. Further packets from outside hosts addressed from the 9.114.11.0 network (the true 9.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 9.114.11.0 0.0.0.255
```

The following example shows NAT configured on the Provider Edge (PE) router with a static route to the shared service for the gold and silver Virtual Private Networks (VPNs). NAT is configured as inside source static one-to-one translations.

```
ip nat pool outside 4.4.4.1 4.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 168.58.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 2.2.2.1 vrf gold
ip nat inside source static 192.169.121.33 2.2.2.2 vrf silver
```

#### Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT), use the **ip nat pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

```
ip nat pool name start-ip end-ip { netmask netmask | prefix-length prefix-length } [type rotary] |
  [accounting list-name]
```

```
no ip nat pool name start-ip end-ip { netmask netmask | prefix-length prefix-length } [type rotary]
  | [accounting list-name]
```

## Syntax Description

<i>name</i>	Name of the pool.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.
<b>netmask</b> <i>netmask</i>	Network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.
<b>prefix-length</b> <i>prefix-length</i>	Number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
<b>type rotary</b>	(Optional) Indicates that the range of addresses in the address pool identifies real, inside hosts among which TCP load distribution will occur.
<b>accounting</b> <i>list-name</i>	(Optional) Indicates the RADIUS profile name that matches the RADIUS configuration in the router.

## Defaults

No pool of addresses is defined.

## Command Modes

Global configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The <b>accounting</b> keyword and <i>list-name</i> argument were added.
12.3(7)T	This command was implemented in Cisco IOS Software Release 12.3(7)T.

## Usage Guidelines

This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define an inside global pool, an outside local pool, or a rotary pool.

## Examples

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
```

```

ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>debug ip nat</b>	Displays information about IP packets translated by NAT.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside source</b>	Enables NAT of the inside destination address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Enables NAT of the outside source address.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.



## ip nat service

To specify a port other than the default port, use the **ip nat service** command in global configuration mode. To disable the port, use the **no** form of this command.

```
ip nat service {H225 | list {access-list-number | access-list-name} {ESP spi-match | IKE preserve-port | ftp tcp port port-number} | ras | rtsp port port-number | sip {tcp | udp} port port-number | skinny tcp port port-number}
```

```
no ip nat service {H225 | list {access-list-number | access-list-name} {ESP spi-match | IKE preserve-port | ftp tcp port port-number} | ras | rtsp port port-number | sip {tcp | udp} port port-number | skinny tcp port port-number}
```

Syntax Description		
<b>H225</b>		H323-H225 protocol.
<b>list</b> <i>access-list-number</i>		Standard access list number in the range from 1 to 199.
<i>access-list-name</i>		Name of a standard IP access list.
<b>ESP</b>		Security Parameter Index (SPI) matching IPsec pass-through.
<b>spi-match</b>		SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
<b>IKE</b>		Preserve Internet Key Exchange (IKE) port, as required by some IPsec servers.
<b>preserve-port</b>		Preserve User Datagram Protocol (UDP) port in IKE packets.
<b>ftp</b>		FTP protocol.
<b>tcp</b>		TCP protocol.
<b>udp</b>		User Datagram Protocol.
<b>port</b> <i>port-number</i>		Port other than the default port in the range from 1 to 65533.
<b>ras</b>		H323-RAS protocol.
<b>rtsp</b>		Real Time Streaming Protocol. This protocol is enabled by default on port 554.
<b>sip</b>		SIP protocol.
<b>skinny</b>		Skinny protocol.

Defaults	
	Disabled
	RTSP is enabled

Command Modes	
	Global configuration

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	The <b>skinny</b> keyword was added.
	12.2(8)T	The <b>sip</b> keyword was added.

Release	Modification
12.2(15)T	The <b>ESP</b> and <b>spi-match</b> keywords were added to enable SPI matching on outside IPsec gateways. The <b>ike</b> and <b>preserve-port</b> keywords were added to enable outside IPsec gateways that require IKE source port 500.
12.3(7)T	The <b>rtsp</b> keyword was added.

### Usage Guidelines

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Use the **no ip nat service rtsp** command to disable support of RTSP packets by NAT. RSTP uses port 554.

### Examples

The following example configures the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example configures the 20002 port of the CallManager:

```
ip nat service skinny tcp port 20002
```

The following example configures TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

The following example configures SPI matching on the endpoint routers:

```
ip nat service list 10 ESP spi-match
```

### Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.

Command	Description
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat stateful id

To designate the members of a translation group, use the **ip nat stateful id** command in global configuration mode.

```
ip nat stateful id id-number { redundancy name / { primary ip-address-primary } { backup ip-address-backup } peer ip-address-peer } mapping-id map-number }
```

```
no ip nat stateful id id-number { redundancy name / { primary ip-address-primary } { backup ip-address-backup } peer ip-address-peer } mapping-id map-number }
```

Syntax Description		
<i>id-number</i>		Unique number given to each router in the stateful translation group.
<b>redundancy</b> <i>name</i>		Establishes Hot Standby Routing Protocol (HSRP) as the method of Redundancy.
<b>primary</b> <i>ip-address-primary</i>		Manually establishes redundancy for the primary router.
<b>backup</b> <i>ip-address-backup</i>		Manually establishes redundancy for the backup router.
<b>peer</b> <i>ip-address-peer</i>		Specifies the ip address of the peer router in the translation group.
<b>mapping-id</b> <i>map-number</i>		Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

**Usage Guidelines** This command has two forms: HSRP stateful NAT translation and manual stateful NAT translation. The form that uses the keyword **redundancy** establishes the HSRP redundancy method. When HSRP mode is set, the primary and backup NAT routers are elected according to the HSRP standby state. To enable stateful NAT manually, configure the primary router and backup router.

**Examples** The following example defines a mapping list that specifies which entries will be forwarded to peers in the group:

```
Router# ip nat stateful id 1

redundancy SNATHSRP
mapping-id 10
mapping-id 11
```

# ip nat translation

The **ip nat translation** command is replaced by the **ip nat translation (timeout)** and **ip nat translation max-entries** commands. See these commands for more information.

# ip nat translation (timeout)

To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

```
ip nat translation { timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout |
icmp-timeout | pptp-timeout | syn-timeout | port-timeout } { seconds | never }
```

```
no ip nat translation { timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout |
icmp-timeout | pptp-timeout | syn-timeout | port-timeout }
```

Syntax Description		
<b>timeout</b>	Specifies that the timeout value applies to dynamic translations except for overload translations. Default is 86,400 seconds (24 hours).	
<b>udp-timeout</b>	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes).	
<b>dns-timeout</b>	Specifies that the timeout value applies to connections to the Domain Name System (DNS). Default is 60 seconds.	
<b>tcp-timeout</b>	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).	
<b>finrst-timeout</b>	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.	
<b>icmp-timeout</b>	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.	
<b>pptp-timeout</b>	Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. Default is 86,400 seconds (24 hours).	
<b>syn-timeout</b>	Specifies the timeout value for TCP flows immediately after a synchronous transmission (SYN) message that consists of digital signals that are sent with precise clocking. The default is 60 seconds.	
<b>port-timeout</b>	Specifies that the timeout value applies to the TCP/UDP port.	
<i>seconds</i>	Number of seconds after which the specified port translation times out. The default is 0.	
<b>never</b>	Specifies no port translation time out.	

## Defaults

```
timeout: 86,400 seconds (24 hours)
udp-timeout: 300 seconds (5 minutes)
dns-timeout: 60 seconds (1 minute)
tcp-timeout: 86,400 seconds (24 hours)
finrst-timeout: 60 seconds (1 minute)
icmp-timeout: 60 seconds (1 minute)
pptp-timeout: 86,400 seconds (24 hours)
syn-timeout: 60 seconds (1 minute)
seconds: 0 (never)
```

## Command Modes

Global configuration

**Command History**

Release	Modification
11.2	This command was introduced.
12.3(4)T	The timeout functions of the <b>ip nat translation</b> command were documented under the command name <b>ip nat translation (timeout)</b> .

**Usage Guidelines**

When port translation is configured, each entry contains more context about the traffic that is using it, which gives you finer control over translation entry timeouts. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless an RST or FIN bit is seen on the stream, in which case they will time out in 1 minute.

**Examples**

The following example configures the router to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
ip nat translation udp-timeout 600
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>ip nat translation max-entries</b>	Limits the maximum number of NAT entries.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat translation max-entries

To limit the size of a Network Address Translation (NAT) table to a specified maximum, use the **ip nat translation max-entries** command in global configuration mode. To remove a specified limit, use the **no** form of this command.

**ip nat translation max-entries** { *number* | **all-vrf** *number* | **host** *ip-address number* | **list** *listname number* | **vrf name** *number* }

**no ip nat translation max-entries** { *number* | **all-vrf** *name number* | **host** *ip-address number* | **list** *listname number* | **vrf name** *number* }

## Syntax Description

<i>number</i>	Maximum number of allowed NAT entries. Range is from 1 to 2147483647.
<b>all-vrf</b>	Constrains each VPN routing and forwarding (VRF) instance by the specified NAT limit.
<b>host</b>	Constrains an IP address by the specified NAT limit.
<i>ip-address</i>	The IP address subject to the NAT limit.
<b>list</b>	Constrains an access control list (ACL) by the specified NAT limit.
<i>listname</i>	The access control list name subject to the NAT limit.
<i>vrf</i>	Constrains an individual VRF instance by the specified NAT limit.
<i>name</i>	The name of the VRF instance subject to the NAT limit.

## Defaults

No maximum size is specified for the NAT table.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Before you configure a NAT rate limit, you should first classify current NAT usage and determine the sources of requests for NAT translations. If a specific host, access control list, or VRF instance is generating an unexpectedly high number of NAT requests, it may be the source of a malicious virus or worm attack.

Once you have identified the source of excess NAT requests, you can set a NAT rate limit that constrains a specific host, access control list, or VRF instance, or you can set a general limit for the maximum number of NAT requests allowed regardless of their source.



### Note

When using the **no** form of **ip nat translation max-entries**, you must specify the type of NAT rate limit you wish to remove and its current value. For more information on how to display current NAT rate limit settings, refer to the **show ip nat statistics** command.



**Examples**

The following examples show how to configure rate limiting NAT translation.

**Setting a General NAT Limit**

The following example shows how to limit the maximum number of allowed NAT entries to 300:

```
Router(config)# ip nat translation max-entries 300
```

**Setting NAT Limits for VRF Instances**

The following example shows how to limit each VRF instance to 200 NAT entries:

```
Router(config)# ip nat translation max-entries all-vrf 200
```

The following example shows how to limit the VRF instance named vrf1 to 150 NAT entries:

```
Router(config)# ip nat translation max-entries vrf vrf1 150
```

The following example shows how to limit the the VRF instance named vrf2 to 225 NAT entries, but limit all other VRF instances to 100 NAT entries each:

```
Router(config)# ip nat translation max-entries all-vrf 100
Router(config)# ip nat translation max-entries vrf vrf2 225
```

**Setting NAT Limits for Access Control Lists**

The following example shows how to limit the access control list named vrf3 to 100 NAT entries:

```
Router(config)# ip nat translation max-entries list vrf3 100
```

**Setting NAT Limits for an IP Address**

The following example shows how to limit the host at IP address 127.0.0.1 to 300 NAT entries:

```
Router(config)# ip nat translation max-entries host 127.0.0.1 300
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>ip nat translation (timeout)</b>	Changes the NAT timeout value.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format** command in line configuration mode. To restore the default display format, use the **no** form of this command.

**ip netmask-format** { **bitcount** | **decimal** | **hexadecimal** }

**no ip netmask-format** [**bitcount** | **decimal** | **hexadecimal**]

Syntax Description	bitcount	decimal	hexadecimal
	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.	Network masks are displayed in dotted-decimal notation (for example, 255.255.255.0).	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0FFFFFF00).

**Defaults** Netmasks are displayed in dotted-decimal format.

**Command Modes** Line configuration

Command History	Release	Modification
	10.3	This command was introduced.

**Usage Guidelines** IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.0 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.0 0FFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.0/24.

**Examples** The following example configures network masks for the specified line to be displayed in bitcount notation in the output of **show** commands:

```
line vty 0 4
 ip netmask-format bitcount
```

## ip nhrp authentication

To configure the authentication string for an interface using the Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication** command in interface configuration mode. To remove the authentication string, use the **no** form of this command.

**ip nhrp authentication** *string*

**no ip nhrp authentication** [*string*]

<b>Syntax Description</b>	<i>string</i>	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long.				
<b>Defaults</b>	No authentication string is configured; the Cisco IOS software adds no authentication option to NHRP packets it generates.					
<b>Command Modes</b>	Interface configuration					
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3	This command was introduced.	
Release	Modification					
10.3	This command was introduced.					
<b>Usage Guidelines</b>	All routers configured with NHRP within one logical NBMA network must share the same authentication string.					
<b>Examples</b>	<p>In the following example, the authentication string named <i>specialxx</i> must be configured in all devices using NHRP on the interface before NHRP communication occurs:</p> <pre>ip nhrp authentication specialxx</pre>					

# ip nhrp holdtime

To change the number of seconds that Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ip nhrp holdtime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip nhrp holdtime** *seconds*

**no ip nhrp holdtime** [*seconds*]

<b>Syntax Description</b>	<i>seconds</i>	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses.
---------------------------	----------------	---

<b>Defaults</b>	7200 seconds (2 hours)
-----------------	------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.3	This command was introduced.

**Usage Guidelines** The **ip nhrp holdtime** command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

**Examples** In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
ip nhrp holdtime 3600
```

# ip nhrp interest

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) request packet, use the **ip nhrp interest** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip nhrp interest** *access-list-number*

**no ip nhrp interest** [*access-list-number*]

<b>Syntax Description</b>	<i>access-list-number</i>	Standard or extended IP access list number in the range from 1 to 199.
---------------------------	---------------------------	--

<b>Defaults</b>	All non-NHRP packets can trigger NHRP requests.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-right: none;">Release</th> <th style="border-left: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-right: none;">10.3</td> <td style="border-left: none;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3	This command was introduced.
Release	Modification				
10.3	This command was introduced.				

<b>Usage Guidelines</b>	<p>Use this command with the <b>access-list</b> command to control which IP packets trigger NHRP requests. The <b>ip nhrp interest</b> command controls <i>which</i> packets cause NHRP address resolution to take place; the <b>ip nhrp use</b> command controls <i>how readily</i> the system attempts such address resolution.</p>
-------------------------	---

<b>Examples</b>	<p>In the following example, any TCP traffic can cause NHRP requests to be sent, but no other IP packets will cause NHRP requests:</p>
-----------------	--

```
ip nhrp interest 101
access-list 101 permit tcp any any
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th style="border-right: none;">Command</th> <th style="border-left: none;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-right: none;"><b>access-list (IP extended)</b></td> <td style="border-left: none;">Defines an extended IP access list.</td> </tr> <tr> <td style="border-right: none;"><b>access-list (IP standard)</b></td> <td style="border-left: none;">Defines a standard IP access list.</td> </tr> <tr> <td style="border-right: none;"><b>ip nhrp use</b></td> <td style="border-left: none;">Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.</td> </tr> </tbody> </table>	Command	Description	<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 nhrp use</b>	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.
Command	Description								
<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 nhrp use</b>	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.								

# ip nhrp map

To statically configure the IP-to-NonBroadcast MultiAccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** interface configuration command. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

**ip nhrp map** *ip-address nbma-address*

**no ip nhrp map** *ip-address nbma-address*

Syntax Description		
	<i>ip-address</i>	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
	<i>nbma-address</i>	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.

**Defaults** No static IP-to-NBMA cache entries exist.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

**Usage Guidelines** You will probably need to configure at least one static mapping in order to reach the Next Hop Server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

**Examples** In the following example, this station in a multipoint tunnel network is statically configured to be served by two Next Hop Servers 100.0.0.1 and 100.0.1.3. The NBMA address for 100.0.0.1 is statically configured to be 11.0.0.1 and the NBMA address for 100.0.1.3 is 12.2.7.8.

```
interface tunnel 0
 ip nhrp nhs 100.0.0.1
 ip nhrp nhs 100.0.1.3
 ip nhrp map 100.0.0.1 11.0.0.1
 ip nhrp map 100.0.1.3 12.2.7.8
```

Related Commands	Command	Description
	<b>clear ip nhrp</b>	Clears all dynamic entries from the NHRP cache.

# ip nhrp map multicast

To configure NonBroadcast MultiAccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** command in interface configuration mode. To remove the destinations, use the **no** form of this command.

**ip nhrp map multicast** *nbma-address*

**no ip nhrp map multicast** *nbma-address*

<b>Syntax Description</b>	<i>nbma-address</i>	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using.
---------------------------	---------------------	--

<b>Defaults</b>	No NBMA addresses are configured as destinations for broadcast or multicast packets.
-----------------	--

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border: none;">Release</th> <th style="border: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border: none;">10.3</td> <td style="border: none;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3	This command was introduced.
Release	Modification				
10.3	This command was introduced.				

<b>Usage Guidelines</b>	<p>This command applies only to tunnel interfaces.</p> <p>The command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the <b>tunnel destination</b> command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.</p> <p>When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.</p>
-------------------------	---

<b>Examples</b>	<p>In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 11.0.0.1 and 11.0.0.2. Addresses 11.0.0.1 and 11.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.</p>
-----------------	--

```
interface tunnel 0
 ip address 10.0.0.3 255.0.0.0
 ip nhrp map multicast 11.0.0.1
 ip nhrp map multicast 11.0.0.2
```

# ip nhrp map multicast dynamic

To allow Next Hop Resolution Protocol (NHRP) to automatically add routers to the multicast NHRP mappings, use the **ip nhrp map multicast dynamic** command in interface configuration mode. To disable this functionality, use the **no** form of this command.

**ip nhrp map multicast dynamic**

**no ip nhrp map multicast dynamic**

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command is not enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

**Usage Guidelines** Use this command when spoke routers need to initiate multipoint generic routing encapsulation (GRE) and IPSEC (IPSec) tunnels and register their unicast NHRP mappings. This command is needed to enable dynamic routing protocols to work over the Multipoint GRE and IPSEC tunnels because IGP routing protocols use multicast packets. This command prevents the Hub router from needing a separate configuration line for a multicast mapping for each spoke router.

**Examples** The following example shows how to enable the **ip nhrp map multicast dynamic** command on the hub router:

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1436
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
```



```
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile vpnprof
!
interface Ethernet0
ip address 172.17.0.1 255.255.255.0
```

# ip nhrp max-send

To change the maximum frequency at which Next Hop Resolution Protocol (NHRP) packets can be sent, use the **ip nhrp max-send** interface configuration command. To restore this frequency to the default value, use the **no** form of this command.

**ip nhrp max-send** *pkt-count* **every** *interval*

**no ip nhrp max-send**

Syntax Description	<i>pkt-count</i>	Number of packets that can be sent in the range from 1 to 65535. Default is 5 packets.
	<b>every</b> <i>interval</i>	Time (in seconds) in the range from 10 to 65535. Default is 10 seconds.

Defaults	<i>pkt-count</i> : 5 packets
	<i>interval</i> : 10 seconds

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

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	The software maintains a per-interface quota of NHRP packets that can be sent. NHRP traffic, whether locally generated or forwarded, cannot be sent at a rate that exceeds this quota. The quota is replenished at the rate specified by the <i>interval value</i> .
------------------	--

Examples	In the following example, only one NHRP packet can be sent from serial interface 0 each minute:
----------	---

```
interface serial 0
 ip nhrp max-send 1 every 60
```

Related Commands	Command	Description
	<b>ip nhrp interest</b>	Controls which IP packets can trigger sending an NHRP request.
	<b>ip nhrp use</b>	Configures the software so that NHRP is deferred until the system has attempted to send data traffic to a particular destination multiple times.

## ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** command in interface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

**ip nhrp network-id** *number*

**no ip nhrp network-id** [*number*]

<b>Syntax Description</b>	<i>number</i>	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
---------------------------	---------------	---

<b>Defaults</b>	NHRP is disabled on the interface.
-----------------	------------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.3	This command was introduced.

<b>Usage Guidelines</b>	In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.
-------------------------	--

<b>Examples</b>	The following example enables NHRP on the interface:
-----------------	--

```
ip nhrp network-id 1
```

# ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs** command in interface configuration mode. To remove the address, use the **no** form of this command.

```
ip nhrp nhs nhs-address [net-address [netmask]]
```

```
no ip nhrp nhs nhs-address [net-address [netmask]]
```

Syntax Description		
<i>nhs-address</i>	Address of the Next Hop Server being specified.	
<i>net-address</i>	(Optional) IP address of a network served by the Next Hop Server.	
<i>netmask</i>	(Optional) IP network mask to be associated with the <i>net</i> IP address. The <i>net</i> IP address is logically ANDed with the mask.	

**Defaults** No Next Hop Servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

**Usage Guidelines** Use this command to specify the address of a Next Hop Server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When Next Hop Servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any Next Hop Server that is configured, you can specify multiple networks that it serves by repeating this command with the same *nhs-address* argument, but with different *net-address* IP network addresses.

**Examples** In the following example, the Next Hop Server with address 131.108.10.11 serves IP network 10.0.0.0. The mask is 255.0.0.0.

```
ip nhrp nhs 131.108.10.11 10.0.0.0 255.0.0.0
```

# ip nhrp record

To reenabling the use of forward record and reverse record options in Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp record** interface configuration command. To suppress the use of such options, use the **no** form of this command.

**ip nhrp record**

**no ip nhrp record**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Forward record and reverse record options are used in NHRP request and reply packets.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

**Usage Guidelines** Forward record and reverse record options provide loop detection and are enabled by default. Using the **no** form of this command disables this method of loop detection. For another method of loop detection, see the **ip nhrp responder** command.

**Examples** The following example suppresses forward record and reverse record options:

```
no ip nhrp record
```

Related Commands	Command	Description
	<b>ip nhrp responder</b>	Designates the primary IP address of which interface the Next Hop Server will use in NHRP reply packets when the NHRP requester uses the Responder Address option.

# ip nhrp registration no-unique

To enable the client to not set the unique flag in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the **ip nhrp registration no-unique** command in interface configuration mode. To reenble this functionality, use the **no** form of this command.

**ip nhrp registration no-unique**

**no ip nhrp registration no-unique**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** This command is not enabled.

---

**Command Modes** Interface configuration

---

Release	Modification
12.3	This command was introduced.

---

---

**Usage Guidelines** If the unique flag is set in the NHRP registration request packet, a Next Hop Server (NHS) must reject any registration attempts for the same private address using a different nonbroadcast multiaccess (NBMA) address. If a client receives a new IP address, for example via DHCP, and tries to register before the cache entry on the NHS times out, the NHS must reject it.

By configuring the **ip nhrp registration no-unique** command, the unique flag is not set, and the NHS can override the old registration information.

This command is useful in an environment where client IP addresses can change frequently such as a dial environment.

---

**Examples** The following example configures the client to not set the unique flag in the NHRP registration packet:

```
interface FastEthernet 0/0
 ip nhrp registration no-unique
```

# ip nhrp responder

To designate the primary IP address the Next Hop Server that an interface will use in Next Hop Resolution Protocol (NHRP) reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder** command in interface configuration mode. To remove the designation, use the **no** form of this command.

**ip nhrp responder** *type number*

**no ip nhrp responder** [*type*] [*number*]

Syntax Description	<i>type</i>	Interface type whose primary IP address is used when a Next Hop Server complies with a Responder Address option (for example, <b>serial or tunnel</b> ).
	<i>number</i>	Interface number whose primary IP address is used when a Next Hop Server complies with a Responder Address option.

**Defaults** The Next Hop Server uses the IP address of the interface where the NHRP request was received.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.

**Usage Guidelines** If an NHRP requestor wants to know which Next Hop Server generates an NHRP reply packet, it can request that information through the Responder Address option. The Next Hop Server that generates the NHRP reply packet then complies by inserting its own IP address in the Responder Address option of the NHRP reply. The Next Hop Server uses the primary IP address of the specified interface.

If an NHRP reply packet being forwarded by a Next Hop Server contains the IP address of that Next Hop Server, the Next Hop Server generates an Error Indication of type “NHRP Loop Detected” and discards the reply packet.

**Examples** In the following example, any NHRP requests for the Responder Address will cause this router acting as a Next Hop Server to supply the primary IP address of serial interface 0 in the NHRP reply packet:

```
ip nhrp responder serial 0
```

# ip nhrp server-only

To configure the interface to operate in Next Hop Resolution Protocol (NHRP) server-only mode, use the **ip nhrp server-only** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**ip nhrp server-only [non-caching]**

**no ip nhrp server-only**

<b>Syntax Description</b>	<b>non-caching</b>	(Optional) The router will not cache NHRP information received on this interface.
---------------------------	--------------------	---

<b>Defaults</b>	Disabled
-----------------	----------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.2	This command was introduced.
12.0	The <b>non-caching</b> keyword was added.	

<b>Usage Guidelines</b>	When the interface is operating in NHRP server-only mode, the interface does not originate NHRP requests or set up an NHRP shortcut Switched Virtual Circuit (SVC).
-------------------------	---

<b>Examples</b>	The following example configures the interface to operate in server-only mode: <pre>ip nhrp server-only</pre>
-----------------	--



# ip nhrp trigger-svc

To configure when the Next Hop Resolution Protocol (NHRP) will set up and tear down a switched virtual circuit (SVC) based on aggregate traffic rates, use the **ip nhrp trigger-svc** command in interface configuration mode. To restore the default thresholds, use the **no** form of this command.

**ip nhrp trigger-svc** *trigger-threshold* *teardown-threshold*

**no ip nhrp trigger-svc**

Syntax Description	<i>trigger-threshold</i>	Average traffic rate calculated during the <b>load interval</b> , at or above which NHRP will set up an SVC for a destination. The default value is 1 kbps.
	<i>teardown-threshold</i>	Average traffic rate calculated during the load interval, at or below which NHRP will tear down the SVC to the destination. The default value is 0 kbps.

Defaults	<i>trigger-threshold</i> : 1 kbps
	<i>teardown-threshold</i> : 0 kbps

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

Command History	Release	Modification
	12.0	This command was introduced.

Usage Guidelines	The two thresholds are measured during a sampling interval of 30 seconds, by default. To change that interval, use the <b>load-interval</b> <i>seconds</i> argument of the <b>ip cef traffic-statistics</b> command.
------------------	--

Examples	In the following example, the triggering and teardown thresholds are set to 100 kbps and 5 kbps, respectively:
----------	--

```
ip nhrp trigger-svc 100 5
```

Related Commands	Command	Description
	<b>ip cef</b>	Enables CEF on the route processor card.
	<b>ip cef accounting</b>	Enables network accounting of CEF information.
	<b>ip cef traffic-statistics</b>	Changes the time interval that controls when NHRP will set up or tear down an SVC.
	<b>ip nhrp interest</b>	Controls which IP packets can trigger sending an NHRP request.

# ip nhrp use

To configure the software so that Next Hop Resolution Protocol (NHRP) is deferred until the system has attempted to send data traffic to a particular destination multiple times, use the **ip nhrp use** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip nhrp use** *usage-count*

**no ip nhrp use** *usage-count*

<b>Syntax Description</b>	<i>usage-count</i>	Packet count in the range from 1 to 65535. Default is 1.
<b>Defaults</b>	<i>usage-count</i> : 1. The first time a data packet is sent to a destination for which the system determines NHRP can be used, an NHRP request is sent.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1	This command was introduced.

**Usage Guidelines**

When the software attempts to send a data packet to a destination for which it has determined that NHRP address resolution can be used, an NHRP request for that destination is normally sent immediately. Configuring the *usage-count* argument causes the system to wait until that many data packets have been sent to a particular destination before it attempts NHRP. The *usage-count* argument for a particular destination is measured over 1-minute intervals (the NHRP cache expiration interval).

The usage count applies *per destination*. So if the *usage-count* argument is configured to be 3, and four data packets are sent toward 10.0.0.1 and one packet toward 10.0.0.2, then an NHRP request is generated for 10.0.0.1 only.

If the system continues to need to forward data packets to a particular destination, but no NHRP response has been received, retransmission of NHRP requests is performed. This retransmission occurs only if data traffic continues to be sent to a destination.

The **ip nhrp interest** command controls *which* packets cause NHRP address resolution to take place; the **ip nhrp use** command controls *how readily* the system attempts such address resolution.

**Examples**

In the following example, if in the first minute five packets are sent to the first destination and five packets are sent to a second destination, then a single NHRP request is generated for the second destination.

If in the second minute the same traffic is generated and no NHRP responses have been received, then the system resends its request for the second destination.

```
ip nhrp use 5
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip nhrp interest</b>	Controls which IP packets can trigger sending an NHRP request.
<b>ip nhrp max-send</b>	Changes the maximum frequency at which NHRP packets can be sent.

# ip options

To drop or ignore IP options packets that are sent to the router, use the **ip options** command in global configuration mode. To disable this functionality and allow all IP options packets to be sent to the router, use the **no** form of this command.

```
ip options {drop | ignore}
```

```
no ip options {drop | ignore}
```

## Syntax Description

<b>drop</b>	Router drops all IP options packets that it receives.
<b>ignore</b>	Router ignores all options and treats the packets as though they did not have any IP options. (The options are not removed from the packet—just ignored.)

## Defaults

This command is not enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

## Usage Guidelines

The **ip options** command allows you to filter IP options packets, mitigating the effects of IP options on the router, and on downstream routers and hosts.

Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and then the ignore mode is configured, the ignore mode will override the drop mode.

## Examples

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
ip options drop
```

```
% Warning:RSVP and other protocols that use IP Options packets may not function in drop or ignore modes.
end
```

# ip proxy-arp

To enable proxy Address Resolution Protocol (ARP) on an interface, use the **ip proxy-arp** command in interface configuration mode. To disable proxy ARP on the interface, use the **no** form of this command.

**ip proxy-arp**

**no ip proxy-arp**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Enabled

---

**Command Modes** Interface configuration

---

Release	Modification
10.0	This command was introduced.

---

---

**Examples** The following example enables proxy ARP on Ethernet interface 0:

```
interface ethernet 0
ip proxy-arp
```

# ip redirects

To enable the sending of Internet Control Message Protocol (ICMP) redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received, use the **ip redirects** command in interface configuration mode. To disable the sending of redirect messages, use the **no** form of this command.

**ip redirects**

**no ip redirects**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled

**Command Modes** Interface configuration

Release	Modification
10.0	This command was introduced.

**Usage Guidelines** Previously, if the Hot Standby Router Protocol (HSRP) was configured on an interface, ICMP redirect messages were disabled by default for the interface. With Cisco IOS Release 12.1(3)T, ICMP redirect messages are enabled by default if HSRP is configured.

**Examples** The following example enables the sending of ICMP redirect messages on Ethernet interface 0:

```
interface ethernet 0
 ip redirects
```

Command	Description
<b>ip default-gateway</b>	Defines a default gateway (router) when IP routing is disabled.
<b>show ip redirects</b>	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

# ip route (global)

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

```
ip route prefix mask {ip-address | interface-type interface-number [ip-address]} [dhcp] [distance]
[name] [permanent] [tag tag]
```

```
no ip route prefix mask
```

## Syntax Description

<i>prefix</i>	IP route prefix for the destination.
<i>mask</i>	Prefix mask for the destination.
<i>ip-address</i>	IP address of the next hop that can be used to reach that network.
<i>interface-type</i> <i>interface-number</i>	Network interface type and interface number.
<b>dhcp</b>	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). <b>Note</b> Specify the <b>dhcp</b> keyword for each routing protocol.
<i>distance</i>	(Optional) An administrative distance.
<i>name</i>	(Optional) Applies a name to the specified route.
<b>permanent</b>	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
<b>tag tag</b>	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.

## Defaults

No static routes are established.

## Command Modes

Global configuration

## Command History

Release	Modification
10.0	This command was introduced.
12.3(8)T	The <b>dhcp</b> keyword was added.
12.3(9)	This command was integrated into Cisco IOS Release 12.3(9) mainline.

## Usage Guidelines

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

## Routing Protocols

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, IGRP-derived routes have a default administrative distance of 100. To have a static route that would be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), and Exterior Gateway Routing Protocol (EIGRP) regardless of whether **redistribute static** commands were specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature.

Also, the target of the static route should be included in the network command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static** command is specified for these protocols. With the following configuration:

```
rtr1 (serial 10.16..188.1/30)-----> rtr2(Fast Ethernet 10.31.1.1/30) ----->

router [rip | eigrp | igrp]
net 10.16..188.0
net 10.31.0.0
```

- RIP and IGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

```
ip route 172.16..188.252 255.255.255.252 FastEthernet0/0
```

RIP and IGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

```
ip route 10.16..188.252 255.255.255.252 s2/1
```

- EIGRP redistributes the route with both of the following commands:

```
ip route 10.16..188.252 255.255.255.252 FastEthernet0/0
```

```
ip route 10.16..188.252 255.255.255.252 s2/1
```

With Open Shortest Path First (OSPF), static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, **ip route 0.0.0.0 0.0.0.0 Ethernet 1/2**) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send ARP requests to any destination addresses that route through the static route.

The practical implication of configuring “**ip route 0.0.0.0 0.0.0.0 Ethernet 1/2**” is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a very large ARP cache (along with attendant memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using Proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example “**ip route 0.0.0.0 0.0.0.0 Ethernet1/2 10.1.2.3**”) with a static route to prevent routes from passing through an unintended interface.



### Static Routes Using a Default DHCP Gateway

With Cisco IOS Release 12.3(8)T, static routes using a default DHCP gateway can be configured. The **dhcp** keyword enables this functionality.

#### Examples

The following example chooses an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed through to a router at 10.31.3.4 if dynamic information with administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 10.31.3.4 110
```



#### Note

Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example routes packets for network 10.31.0.0 to a router at 10.31.6.6:

```
ip route 10.31.0.0 255.255.0.0 10.31.6.6
```

The following example routes packets for network 10.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 10.168.1.0 255.255.0.0 Ethernet0 10.1.2.3
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 209.165.200.225 255.255.255.255 ether1 dhcp
ip route 209.165.200.226 255.255.255.255 ether2 dhcp 20
```

#### Related Commands

Command	Description
<b>show ip route</b>	Displays the state of the routing table

# ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no** form of this command.

**ip routing**

**no ip routing**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Enabled

---

**Command Modes** Global configuration

---

Release	Modification
10.0	This command was introduced.

---

---

**Usage Guidelines** To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging to bridge IP.

The ip routing command is disabled on the Cisco VG200 voice over IP gateway.

---

**Examples** The following example enables IP routing:

```
ip routing
```

# ip slb dfp

To configure the Dynamic Feedback Protocol (DFP) and supply an optional password, use the **ip slb dfp** command in global configuration mode. To remove the DFP configuration, use the **no** form of this command.

**ip slb dfp** [**password** *password* [*timeout*]]

**no ip slb dfp**

## Syntax Description

<b>password</b>	(Optional) Specifies a password for MD5 authentication.
<i>password</i>	(Optional) Password value for MD5 authentication. This password must match the password configured on the host agent.
<i>timeout</i>	(Optional) Delay period (in seconds) during which both the old password and the new password are accepted. The default value is 180 seconds.

## Defaults

The password timeout default is 180 seconds.

## Command Modes

Global 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.

## Usage Guidelines

The optional password, if configured, must match the password configured on the host agent.

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

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

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

## Examples

The following example configures DFP, sets the password to flounder, configures a timeout period of 60 seconds, and changes to DFP configuration mode:

```
ip slb dfp flounder 60
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>agent</b>	Configures a DFP agent.

# ip slb serverfarm

To identify a server farm and enter SLB server farm configuration mode, use the **ip slb serverfarm** command in global configuration mode. To remove the server farm from the IOS SLB configuration, use the **no** form of this command.

**ip slb serverfarm** *serverfarm-name*

**no ip slb serverfarm** *serverfarm-name*

<b>Syntax Description</b>	<i>serverfarm-name</i>	Character string used to identify the server farm. The character string is limited to 15 characters.
---------------------------	------------------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

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

**Examples** The following example identifies a server farm named PUBLIC:

```
ip slb serverfarm PUBLIC
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>real</b>	Identifies a real server.

# ip slb vserver

To identify a virtual server and enter SLB virtual server configuration mode, use the **ip slb vserver** command in global configuration mode. To remove a virtual server from the IOS SLB configuration, use the **no** form of this command.

**ip slb vserver** *virtserver-name*

**no ip slb vserver** *virtserver-name*

<b>Syntax Description</b>	<i>virtserver-name</i>	Character string used to identify the virtual server. The character string is limited to 15 characters.
---------------------------	------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

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

**Examples** The following example identifies a virtual server named PUBLIC\_HTTP:

```
ip slb vserver PUBLIC_HTTP
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>serverfarm</b>	Associates a real server farm with a virtual server.
	<b>show ip slb vservers</b>	Displays information about the virtual servers.

# ip source-route

To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the **ip source-route** command in global configuration mode. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

**ip source-route**

**no ip source-route**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled

**Command Modes** Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Examples** The following example enables the handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands	Command	Description
	<b>ping (privileged)</b>	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
	<b>ping (user)</b>	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

# ip subnet-zero

To enable the use of subnet 0 for interface addresses and routing updates, use the **ip subnet-zero** command in global configuration mode. To restore the default, use the **no** form of this command.

**ip subnet-zero**

**no ip subnet-zero**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Enabled

---

**Command Modes** Global configuration

---

Release	Modification
10.0	This command was introduced.

---

---

**Usage Guidelines** The **ip subnet-zero** command provides the ability to configure and route to subnet 0 subnets. Subnetting with a subnet address of 0 is discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

---

**Examples** The following example enables subnet zero:

```
ip subnet-zero
```



# ip tcp chunk-size

To alter the TCP maximum read size for Telnet or rlogin, use the **ip tcp chunk-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

**ip tcp chunk-size** *characters*

**no ip tcp chunk-size**

<b>Syntax Description</b>	<i>characters</i>	Maximum number of characters that Telnet or rlogin can read in one read instruction. The default value is 0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.
---------------------------	-------------------	--

<b>Defaults</b>	0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.
-----------------	--

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	9.1	This command was introduced.

<b>Usage Guidelines</b>	It is unlikely you will need to change the default value.
-------------------------	---

<b>Examples</b>	The following example sets the maximum TCP read size to 64,000 bytes: <pre>ip tcp chunk-size 64000</pre>
-----------------	---

# ip tcp ecn

To enable TCP Explicit Congestion Notification (ECN), use the **ip tcp ecn** command in global configuration mode. To disable TCP ECN, use the **no** form of this command.

**ip tcp ecn**

**no ip tcp ecn**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** TCP ECN is disabled.

---

**Command Modes** Global configuration

---

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

---

---

**Examples** The following example shows you how to enable TCP ECN:

```
ip tcp ecn
```

---

Command	Description
<b>debug ip tcp ecn</b>	Turns on TCP ECN debugging.
<b>show tcp tcb</b>	Displays the status of local and remote end hosts.

---

# ip tcp mss

To enable a maximum segment size (MSS) for TCP connections originating or terminating on a router, use the **ip tcp mss command** in global configuration mode. To disable the configuration of the MSS, use the **no** form of this command.

**ip tcp mss** *mss-value*

**no ip tcp mss** *mss-value*

<b>Syntax Description</b>	<i>mss-value</i>	Maximum segment size for TCP connections in bytes. The range is from 68 to 1000.
---------------------------	------------------	--

<b>Defaults</b>	This command is disabled.
-----------------	---------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(05)S	This command was introduced.
	12.1	This command was integrated into Cisco IOS Release 12.1.

**Usage Guidelines** If this command is not enabled, the MSS value of 536 bytes is used if the destination is not on a LAN, otherwise the MSS value is 1460 for a local destination.

For connections originating from a router, the specified value is used directly as an MSS option in the synchronize (SYN) segment. For connections terminating on a router, the value is used only if the incoming SYN segment has an MSS option value higher than the configured value. Otherwise the incoming value is used as the MSS option in the SYN/acknowledge (ACK) segment.



### Note

The **ip tcp mss** command interacts with the **ip tcp path-mtu-discovery** command and not the **ip tcp header-compression** command. The **ip tcp path-mtu-discovery** command changes the default MSS to 1460 even for non-local nodes.

**Examples** The following example sets the MSS value at 250:

```
ip tcp mss 250
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip tcp header-compression</b>	Specifies the total number of header compression connections that can exist on an interface.

## ip tcp path-mtu-discovery

To enable the Path MTU Discovery feature for all new TCP connections from the router, use the **ip tcp path-mtu-discovery** command in global configuration mode. To disable the function, use the **no** form of this command.

```
ip tcp path-mtu-discovery [age-timer {minutes | infinite}]
```

```
no ip tcp path-mtu-discovery [age-timer {minutes | infinite}]
```

### Syntax Description

<b>age-timer</b> <i>minutes</i>	(Optional) Time interval (in minutes) after which TCP re-estimates the path MTU with a larger maximum segment size (MSS). The maximum is 30 minutes; the default is 10 minutes.
<b>age-timer infinite</b>	(Optional) Turns off the age timer.

### Defaults

Disabled. If enabled, the default *minutes* value is 10 minutes.

### Command Modes

Global configuration

### Command History

Release	Modification
10.3	This command was introduced.
11.2	The <b>age-timer</b> and <b>infinite</b> keywords were added.

### Usage Guidelines

Path MTU Discovery is a method for maximizing the use of available bandwidth in the network between the endpoints of a TCP connection. It is described in RFC 1191. Existing connections are not affected when this feature is turned on or off.

Customers using TCP connections to move bulk data between systems on distinct subnets would benefit most by enabling this feature.

The age timer is a time interval for how often TCP re-estimates the path MTU with a larger MSS. When the age timer is used, TCP path MTU becomes a dynamic process. If the MSS used for the connection is smaller than what the peer connection can handle, a larger MSS is tried every time the age timer expires. The discovery process is stopped when either the send MSS is as large as the peer negotiated, or the user has disabled the timer on the router. You can turn off the age timer by setting it to infinite.

### Examples

The following example enables Path MTU Discovery:

```
ip tcp path-mtu-discovery
```

# ip tcp queuemax

To alter the maximum TCP outgoing queue per connection, use the **ip tcp queuemax** command in global configuration mode. To restore the default value, use the **no** form of this command.

**ip tcp queuemax** *packets*

**no ip tcp queuemax**

<b>Syntax Description</b>	<i>packets</i>	Outgoing queue size of TCP packets. The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.
<b>Defaults</b>	The default value is 5 segments if the connection has a TTY associated with it. If no TTY is associated with it, the default value is 20 segments.	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
<b>Usage Guidelines</b>	Changing the default value changes the 5 segments, not the 20 segments.	
<b>Examples</b>	The following example sets the maximum TCP outgoing queue to 10 packets: <pre>ip tcp queuemax 10</pre>	

# ip tcp selective-ack

To enable TCP selective acknowledgment, use the **ip tcp selective-ack** command in global configuration mode. To disable TCP selective acknowledgment, use the **no** form of this command.

**ip tcp selective-ack**

**no ip tcp selective-ack**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Disabled

**Command Modes** Global configuration

Command History	Release	Modification
	11.2 F	This command was introduced.

**Usage Guidelines** TCP might not experience optimal performance if multiple packets are lost from one window of data. With the limited information available from cumulative acknowledgments, a TCP sender can learn about only one lost packet per round-trip time. An aggressive sender could resend packets early, but such re-sent segments might have already been received.

The TCP selective acknowledgment mechanism helps overcome these limitations. The receiving TCP returns selective acknowledgment packets to the sender, informing the sender about data that has been received. The sender can then resend only the missing data segments.

TCP selective acknowledgment improves overall performance. The feature is used only when a multiple number of packets drop from a TCP window. There is no performance impact when the feature is enabled but not used.

This command becomes effective only on new TCP connections opened after the feature is enabled.

This feature must be disabled if you want TCP header compression. You might disable this feature if you have severe TCP problems.

Refer to RFC 2018 for more detailed information on TCP selective acknowledgment.

**Examples** The following example enables the router to send and receive TCP selective acknowledgments:

```
ip tcp selective-ack
```

Related Commands	Command	Description
	<b>ip tcp header-compression</b>	Enables TCP header compression.

# ip tcp synwait-time

To set a period of time the Cisco IOS software waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** command in global configuration mode. To restore the default time, use the **no** form of this command.

**ip tcp synwait-time** *seconds*

**no ip tcp synwait-time** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Time (in seconds) the software waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds. The default is 30 seconds.
---------------------------	----------------	---

<b>Defaults</b>	The default time is 30 seconds.
-----------------	---------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	<p>In versions previous to Cisco IOS software Release 10.0, the system would wait a fixed 30 seconds when attempting to establish a TCP connection. If your network contains public switched telephone network (PSTN) dial-on-demand routing (DDR), the call setup time may exceed 30 seconds. This amount of time is not sufficient in networks that have dialup asynchronous connections because it will affect your ability to Telnet over the link (from the router) if the link must be brought up. If you have this type of network, you may want to set this value to the UNIX value of 75.</p>
-------------------------	--

Because this is a host parameter, it does not pertain to traffic going *through* the router, just for traffic originated *at* this device. Because UNIX has a fixed 75-second timeout, hosts are unlikely to experience this problem.

<b>Examples</b>	The following example configures the Cisco IOS software to continue attempting to establish a TCP connection for 180 seconds:
-----------------	---

```
ip tcp synwait-time 180
```

# ip tcp timestamp

To enable TCP time stamp, use the **ip tcp timestamp** command in global configuration mode. To disable TCP time stamp, use the **no** form of this command.

**ip tcp timestamp**

**no ip tcp timestamp**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Release	Modification
11.2 F	This command was introduced.

---

---

**Usage Guidelines** TCP time stamp improves round-trip time estimates. Refer to RFC 1323 for more detailed information on TCP time stamp.

The TCP time stamp must be disabled if you want to use TCP header compression.

---

**Examples** The following example enables the router to send TCP time stamps:

```
ip tcp timestamp
```

---

Command	Description
<b>ip tcp header-compression</b>	Enables TCP header compression.

---



# ip tcp window-size

To alter the TCP window size, use the **ip tcp window-size** command in global configuration mode. To restore the default value, use the **no** form of this command.

**ip tcp window-size** *bytes*

**no ip tcp window-size**

<b>Syntax Description</b>	<i>bytes</i>	Window size (in bytes). An integer from 0 to 1,073,741,823. The default value is 4128 bytes. Window scaling is enabled when the window size is greater than 65,535 bytes.
---------------------------	--------------	---

<b>Defaults</b>	The default window size is 4128 bytes when window scaling is not enabled. If only one neighbor is configured for the window scaling extension, the default window size is 65,535 bytes.
-----------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	9.1	This command was introduced.
12.2(8)T	Default window size and maximum window scaling factor were increased.	

<b>Usage Guidelines</b>	<p>Do not use this command unless you clearly understand why you want to change the default value.</p> <p>To enable window scaling to support Long Fat Networks (LFNs), the TCP window size must be more than 65,535 bytes. The remote side of the link also needs to be configured to support window scaling. If both sides are not configured with window scaling, the default maximum value of 65,535 bytes is applied.</p> <p>The scale factor is automatically calculated based on the window-size you configure. You cannot directly configure the scale factor.</p>
-------------------------	--

<b>Examples</b>	<p>The following example sets the TCP window size to 1000 bytes:</p> <pre>ip tcp window-size 1000</pre>
-----------------	---

# ip unnumbered

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

**ip unnumbered** *type number*

**no ip unnumbered** *type number*

<b>Syntax Description</b>	<i>type number</i>	Type and number of another interface on which the router has an assigned IP address. The interface cannot be another unnumbered interface.
---------------------------	--------------------	--

<b>Defaults</b>	Disabled
-----------------	----------

<b>Command Modes</b>	Interface configuration Subinterface configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
	12.3(4)T	This command was modified to configure IP unnumbered support on Ethernet VLAN subinterfaces and subinterface ranges.

**Usage Guidelines** Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions are as follows:

- Serial interfaces using High Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP) and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping EXEC** command to determine whether the interface is up, because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- You cannot netboot a runnable image over an unnumbered serial interface.
- You cannot support IP security options on an unnumbered interface.

The interface you specify by the *type* and *number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered. This configuration allows you to comply with RFC 1195, which states that IP addresses are not required on each interface.

**Note**

---

Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, then any routing protocol running across the serial line must not advertise subnet information.

---

---

**Examples**

In the following example, the first serial interface is given the address of Ethernet 0:

```
interface ethernet 0
 ip address 131.108.6.6 255.255.255.0
!
interface serial 0
 ip unnumbered ethernet 0
```

In the following example, Ethernet VLAN subinterface 3/0.2 is configured as an IP unnumbered subinterface:

```
interface ethernet 3/0.2
 encapsulation dot1q 200
 ip unnumbered ethernet 3/1
```

In the following example, Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 are configured as IP unnumbered subinterfaces:

```
interface range fastethernet5/1.1 - fastethernet5/1.4
 ip unnumbered ethernet 3/1
```

# ip unreachable

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachable** command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip unreachable**

**no ip unreachable**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** Enabled

---

**Command Modes** Interface configuration

---

Release	Modification
10.0	This command was introduced.

---

---

**Usage Guidelines** If the Cisco IOS software receives a nonbroadcast packet destined for itself that uses a protocol it does not recognize, it sends an ICMP unreachable message to the source.

If the software receives a datagram that it cannot deliver to its ultimate destination because it knows of no route to the destination address, it replies to the originator of that datagram with an ICMP host unreachable message.

This command affects all types of ICMP unreachable messages.

---

**Examples** The following example enables the generation of ICMP unreachable messages, as appropriate, on an interface:

```
interface ethernet 0
 ip unreachable
```

## ip vrf (tracking)

To configure a VPN routing and forwarding (VRF) table, use the **ip vrf** command in tracking configuration mode. To remove a VRF table, use the **no** form of this command.

**ip vrf** *vrf-name*

**no ip vrf** *vrf-name*

<b>Syntax Description</b>	<i>vrf-name</i>	Name assigned to a VRF.
---------------------------	-----------------	-------------------------

<b>Defaults</b>	The VRF table is not configured.
-----------------	----------------------------------

<b>Command Modes</b>	Tracking configuration
----------------------	------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.	

<b>Usage Guidelines</b>	This command is available for all IP-route tracked objects that are tracked by the <b>track ip route</b> global configuration command. Use this command to track a route that belongs to a specific VPN.
-------------------------	--

<b>Examples</b>	In the following example, the route associated with a VRF named VRF1 is tracked:
-----------------	--

```
track 1 ip route 10.0.0. 255.255.255.0.0 reachability
 ip vrf VRF1
 rd 100:1
 route-target both 100:1
!
interface e0/2
 no shutdown
 ip vrf forwarding VRF1
 ip address 20.0.0.2 255.0.0.0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>track ip route</b>	Tracks the state of an IP route and enters tracking configuration mode.

# ip wccp

To allocate space and to enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **ip wccp** command in global configuration mode. To disable the service group and deallocate space, use the **no** form of this command.

```
ip wccp { web-cache | service-number / outbound-acl-check } [group-address multicast-address]
[redirect-list access-list] [group-list access-list] [password password [0 | 7]]
```

```
no ip wccp { web-cache | service-number } [group-address multicast-address] [redirect-list
access-list] [group-list access-list] [password password [0 | 7]]
```

## Syntax Description

<b>web-cache</b>	Enables the web-cache service, WCCP version 1 and version 2.
<i>service-number</i>	Enables WCCP, version 1 only. The service number is dynamic, which means the service definition is dictated by the cache. The range is from 0 to 255. If Cisco Cache Engines are being used in your service group, the <b>reverse-proxy</b> service is indicated by a value of 99.
<b>outbound-acl-check</b>	Enables the outbound access control list (ACL) check. <b>Note</b> This keyword must be specified alone.
<b>group-address</b> <i>multicast-address</i>	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. The <i>multicast-address</i> argument requires a multicast address, which is used by the router to determine which web cache should receive redirected messages.
<b>redirect-list</b> <i>access-list</i>	(Optional) Directs the router to use an access list to control traffic redirected to this service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
<b>group-list</b> <i>access-list</i>	(Optional) Directs the router to use an access list to determine which web caches are allowed to participate in the service group. The <i>access-list</i> argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
<b>password</b> <i>password</i>	(Optional) Directs the router to apply Message Digest 5 (MD5) authentication to messages received from the service group. Messages that are not accepted by the authentication are discarded. The password can be up to seven characters in length.
<b>0</b>   <b>7</b>	(Optional) Indicates the HMAC MD5 algorithm used to encrypt a password created for a cache engine.

## Defaults

WCCP services are not enabled on the router.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command replaced the <b>ip wccp enable</b> , <b>ip wccp redirect-list</b> , and <b>ip wccp group-list</b> commands.
12.3(7)T	The <b>outbound-acl-check</b> keyword was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

## Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

This command instructs a router to enable or disable the support for the specified service number or the web-cache service name. A service number can be from 0 to 99. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still have the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once. The following sections outline the specific usage of each of the optional forms of this command.

**ip wccp** { **web-cache** | *service-number* } **group-address** *multicast-address*

A WCCP group address can be configured to set up a multicast address that cooperating routers and web caches can use to exchange WCCP protocol messages. If such an address is used, IP multicast routing must be enabled so that the messages that use the configured group (multicast) addresses are received correctly.

This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. The response is sent to the group address as well. The default is for no group address to be configured, in which case all “Here I Am” messages are responded to with a unicast reply.

**ip wccp** { **web-cache** | *service-number* } **redirect-list** *access-list*

This option instructs the router to use an access list to control the traffic that is redirected to the web caches of the service group specified by the service name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number or a name to represent a named standard access list. The access list itself specifies which traffic is permitted to be redirected. The default is for no redirect list to be configured (all traffic is redirected).

WCCP requires that the following protocol and ports not be filtered by any access lists:

- User Datagram Protocol (UDP) (protocol type 17) port 2048. This port is used for control signaling. Blocking this type of traffic will prevent WCCP from establishing a connection between the router and web caches.
- Generic routing encapsulation (GRE) (protocol type 47 encapsulated frames). Blocking this type of traffic will prevent the web caches from ever seeing the packets that are intercepted.

**ip wccp** {web-cache | service-number} **group-list** access-list

This option instructs the router to use an access list to control the web caches allowed to participate in the specified service group. The *access-list* parameter specifies either a number from 1 to 99 to represent a standard access list number or a name to represent a named standard access list. The access list itself specifies which web caches are permitted to participate in the service group. The default is for no group list to be configured, in which case all web caches may participate in the service group.



#### Note

The **ip wccp** {web-cache | service-number} **group-list** command syntax resembles the **ip wccp** {web-cache | service-number} **group-listen** command, but these are entirely different commands. The **ip wccp group-listen** command is an interface configuration command used to configure an interface to listen for multicast notifications from a cache cluster. Refer to the description of the **ip wccp group-listen** command in the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services, Release 12.3 T*.

**ip wccp** {web-cache | service-number} **password** password

This option instructs the router to use MD5 authentication on the messages received from the service group specified by the service name given. Use this form of the command to set the password on the router. You must also configure the same password separately on each web cache. The password can be up to a maximum of seven characters. Messages that do not authenticate when authentication is enabled on the router are discarded. The default is for no authentication password to be configured and for authentication to be disabled.

#### Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 10.1.1.1:

```
ip wccp 99 group-address 10.1.1.1
interface ethernet 0
 ip wccp web-cache group-list
```

The following example shows how to configure a router to redirect web-related packets without a destination of 10.168.196.51 to the web cache:

```
access-list 100 deny ip any host 10.168.196.51
access-list 100 permit ip any any
ip wccp web-cache redirect-list 100
interface Ethernet 0
 ip web-cache redirect-list
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving interface f0/0. Because the outbound ACL check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
ip wccp web-cache
ip wccp outbound-acl-check
```



```
interface f0/0
 ip access-group 10 out
 ip wccp web-cache redirect-list out
 access-list 10 deny 10.0.0.0 0.255.255.255
 access-list 10 permit any
```

If the outbound ACL check is disabled, HTTP packets from network 10.0.0.0 would be redirected to a cache and users with that network address could retrieve web pages when the network administrator wanted to prevent this from happening.

---

**Related Commands**

Command	Description
<b>ip wccp check services all</b>	Enables all Web Cache Communication Protocol (WCCP) services.
<b>ip wccp version</b>	Specifies which version of WCCP you wish to use on your router.

## ip wccp enable

The **ip wccp enable** has been replaced by the **ip wccp** command. See the description of the **ip wccp** command in this chapter for more information.

# ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for the Web Cache Communication Protocol (WCCP) feature, use the **ip wccp group-listen** command in interface configuration mode. To remove control of the reception of IP multicast packets for the WCCP feature, use the **no** form of this command.

**ip wccp {web-cache | service-number} group-listen**

**no ip wccp {web-cache | service-number} group-listen**

## Syntax Description

<b>web-cache</b>	Directs the router to send packets to the web cache service.
<i>service-number</i>	The identification number of the cache engine service group being controlled by a router. The number can be from 0 to 99.

## Defaults

This command is disabled by default.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(3)T	This command was introduced.

## Usage Guidelines

On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required:

- The IP multicast address for use by the WCCP Service Group must be configured.
- The interfaces on which the router wishes to receive the IP multicast address to be configured with the **ip wccp {web-cache | service-number} group-listen** interface configuration command.

## Examples

In the following example, a user enables the multicast packets for a web cache with a multicast address of 224.1.1.100.

```
ip wccp web-cache group-address 224.1.1.100
interface ethernet 0
ip wccp web-cache group listen
```

## Related Commands

Command	Description
<b>ip wccp</b>	Directs a router to enable or disable the support for a WCCP cache engine service group.
<b>ip wccp redirect</b>	Enables WCCP redirection on an interface.

# ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp service redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

```
ip wccp service redirect {out | in}
```

```
no ip wccp service redirect {out | in}
```

## Syntax Description

<i>service</i>	Specifies the service group. You can specify the <b>web-cache</b> keyword, or you can specify the identification number (from 0 to 99) of the service.
<b>redirect</b>	Enables packet redirection checking on an outbound or inbound interface.
<b>out</b>	Specifies packet redirection on an outbound interface.
<b>in</b>	Specifies packet redirection on an inbound interface.

## Defaults

Redirection checking on the interface is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(3) T	This command was introduced.
12.0(11)S	The <b>in</b> keyword was added to the 12.0 S release train.
12.1(3)T	The <b>in</b> keyword was added to the 12.1 T release train.

## Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

The **ip wccp service redirect in** command allows you to configure WCCP redirection on an interface receiving inbound network traffic. When the command is applied to an interface, all packets arriving at that interface will be compared against the criteria defined by the specified WCCP service. If the packets match the criteria, they will be redirected.

Likewise, the **ip wccp service redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

**Tips**

Be careful not to confuse the **ip wccp service redirect {out | in}** interface configuration command with the **ip wccp redirect exclude in** interface configuration command.

**Note**

This command has the potential to effect the **ip wccp redirect exclude in** command. (These commands have opposite functions.) If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp service redirect in** command, the “exclude in” command will be overridden. The opposite is also true: configuring the “exclude in” command will override the “redirect in” command.

**Examples**

In the following example, the user configures a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect ?
    in   Redirect to a Cache Engine appropriate inbound packets
    out  Redirect to a Cache Engine appropriate outbound packets
Router(config-if)# ip wccp 99 redirect out
```

In the following example, the user configures a session in which HTTP traffic arriving on Ethernet interface 0/1 will be redirected to a Cisco Cache Engine:

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

**Related Commands**

Command	Description
<b>ip wccp redirect exclude in</b>	Enables redirection exclusion on an interface.

# ip wccp redirect exclude in

To configure an interface to exclude packets received on an interface from being checked for redirection, use the **ip wccp redirect exclude in** command in interface configuration mode. To disable the ability of a router to exclude packets from redirection checks, use the **no** form of this command.

**ip wccp redirect exclude in**

**no ip wccp redirect exclude in**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Redirection exclusion is disabled.

**Command Modes** Interface configuration

Release	Modification
12.0(3)T	This command was introduced.

**Usage Guidelines** WCCP transparent caching bypasses Network Address Translation (NAT) when fast (Cisco Express Forwarding [CEF]) switching is enabled. To work around this situation, WCCP transparent caching should be configured in the outgoing direction, fast/CEF switching enabled on the Content Engine interface, and the **ip wccp web-cache redirect out** command specified. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group and the specified redirect list will deny packets with a NAT (source) IP address and prevent redirection. Refer to the **ip wccp** command for configuration of the redirect list and service group.

This configuration command instructs the interface to exclude inbound packets from any redirection check that may occur at the outbound interface. Note that the command is global to all the services and should be applied to any inbound interface that you wish to exclude from redirection.

This command is intended to be used to accelerate the flow of packets from a cache engine to the internet as well as allow for the use of the WCCPv2 Packet Return feature.

**Examples** In the following example, packets arriving on Ethernet interface 0 are excluded from all WCCP redirection checks:

```
Router(config)# interface ethernet 0
Router(config-if)# ip wccp redirect exclude in
```

**ip wccp redirect exclude in**

Related Commands	Command	Description
	<b>ip wccp</b>	Directs a router to enable or disable the support for a cache engine service group.
	<b>ip wccp redirect out</b>	Configures an interface to enable a the ability of a router to verify that appropriate packets are being redirected to a cache engine.

## ip wccp redirect-list

This command is now documented as part of the **ip wccp** { **web-cache** | *service-number* } command. See the description of the **ip wccp** command in this book for more information.



# ip wccp version

To specify which version of Web Cache Communication Protocol (WCCP) you wish to configure on your router, use the **ip wccp version** command in global configuration mode.

**ip wccp version {1 | 2}**

Syntax Description	1	Web Cache Communication Protocol Version 1 (WCCPv1).
	2	Web Cache Communication Protocol Version 2 (WCCPv2).

**Defaults** WCCPv2

**Command Modes** Global configuration

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

**Examples** In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1, starting in privileged EXEC mode:

```
router# show ip wccp
% WCCP version 2 is not enabled
router# configure terminal
router(config)# ip wccp version 1
router(config)# end
router# show ip wccp
% WCCP version 1 is not enabled
```

## ip web-cache redirect

The **ip web-cache redirect** interface configuration command has been replaced by the **ip wccp redirect** interface configuration command. The **ip web-cache redirect** command is no longer supported. See the description of the **ip wccp redirect** command in this book for more information.

# lease

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

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

**no lease**

## Syntax Description

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

## Defaults

1 day

## Command Modes

DHCP pool configuration

## Command History

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

## Examples

The following example shows a 1-day lease:

```
lease 1
```

The following example shows a 1-hour lease:

```
lease 0 1
```

The following example shows a 1-minute lease:

```
lease 0 0 1
```

The following example shows an infinite (unlimited) lease:

```
lease infinite
```

## Related Commands

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

## local-ip (IPC transport-SCTP local)

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

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

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

### Syntax Description

<i>device-real-ip-address</i>	IP address of the local device.  The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in global Virtual Routing and Forwarding (VRF). A virtual IP (VIP) address cannot be used.
<i>device-real-ip-address2</i>	(Optional) IP address of the local device.

### Defaults

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

### Command Modes

IPC transport-SCTP local configuration

### Command History

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

### Usage Guidelines

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

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

### Examples

The following example shows how to enable SSO:

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

## ■ local-ip (IPC transport-SCTP local)

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

# local-port

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

**local-port** *local-port-number*

## Syntax Description

<i>local-port-number</i>	Local port number, which should be the same as the remote port number on the peer router (which is specified via the <b>remote-port</b> command).
--------------------------	---

## Defaults

A local SCTP port is not defined.

## Command Modes

SCTP protocol configuration

## Command History

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

## Usage Guidelines

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

## Examples

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

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

## Related Commands

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

## manager (DFP agent)

This command has been replaced by the following commands:

Command in Cisco IOS Release 12.1(8a)E	Replacement Commands in Cisco IOS Releases 12.2(14)S and 12.3(4)T
<b>manager</b>	<b>inservice (DFP agent)</b> <b>interval (DFP agent)</b> <b>ip dfp agent</b> <b>password (DFP agent)</b> <b>port (DFP agent)</b>

# maxconns

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

**maxconns** *maximum-number*

**no maxconns**

<b>Syntax Description</b>	<i>maximum-number</i>	Maximum number of simultaneous active connections on the real server. Valid values range from 1 to 4294967295. The default is 4294967295.
<b>Defaults</b>	The default maximum number is 4294967295.	
<b>Command Modes</b>	SLB real server configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(7)XE	This command was introduced.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
<b>Examples</b>	The following example limits the real server to a maximum of 1000 simultaneous active connections:	
	<pre>ip slb serverfarm PUBLIC real 10.10.1.1 maxconns 1000</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>real</b>	Identifies a real server.
	<b>show ip slb reals</b>	Displays information about the real servers.
	<b>show ip slb severfarms</b>	Displays information about the server farm configuration.



# nat

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

**nat server**

**no nat server**

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

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	SLB server farm configuration
----------------------	-------------------------------

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

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

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

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

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

# netbios-name-server

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

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

**no netbios-name-server**

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

**Command Modes** DHCP pool configuration

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

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

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

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

Related Commands	Command	Description
	<b>dns-server</b>	Specifies the DNS IP servers available to a DHCP client.
	<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.
	<b>netbios-node-type</b>	Configures the NetBIOS node type for Microsoft DHCP clients.

# netbios-node-type

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

**netbios-node-type** *type*

**no netbios-node-type**

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

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Usage Guidelines</b>	The recommended type is h-node (hybrid).
-------------------------	--

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

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

## network (DHCP)

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

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

**no network**

### Syntax Description

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

### Defaults

No default behavior or values.

### Command Modes

DHCP pool configuration

### Command History

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

### Usage Guidelines

This command is valid for DHCP subnetwork address pools only. If the mask or prefix length is not specified, the class A, B, or C natural mask is used. The DHCP Server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the **ip dhcp excluded-address** command.

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

### Examples

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

```
network 172.16.0.0/16
```

### Related Commands

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

Command	Description
<b>ip dhcp excluded-address</b>	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

## next-server

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

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

**no next-server** *address*

### Syntax Description

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

### Defaults

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

### Command Modes

DHCP pool configuration

### Command History

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

### Usage Guidelines

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

### Examples

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

```
next-server 10.12.1.99
```

### Related Commands

Command	Description
<b>accounting (DHCP)</b>	Specifies the name of the default boot image 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.
<b>ip helper-address</b>	Forwards UDP broadcasts, including BOOTP, received on an interface.
<b>option</b>	Configures Cisco IOS DHCP server options.

# no ip gratuitous-arps

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

**no ip gratuitous-arps**

---

**Syntax Description** This command has no keywords or arguments.

---

**Defaults** Disabled

---

**Command Modes** Global configuration

---

Release	Modification
11.3	This command was introduced.

---

---

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

---

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

```
no ip gratuitous-arps
```

## object (tracking)

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

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

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

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

**Defaults** The object is removed from the tracked list.

**Command Modes** Tracking configuration

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

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

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

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

Related Commands	Command	Description
	<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.



# option

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

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

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

Syntax Description		
	<i>code</i>	Specifies the DHCP option code.
	<b>instance</b> <i>number</i>	(Optional) Specifies a number from 0 to 255.
	<b>ascii</b> <i>string</i>	Specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks.
	<b>hex</b> <i>string</i>	Specifies dotted hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits—each byte can be separated by a period, colon, or white space.
	<b>ip</b> <i>address</i>	Specifies an IP address.

**Defaults** The default instance number is 0.

**Command Modes** DHCP pool configuration

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

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

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

```
option 19 hex 01
```

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

```
option 72 ip 172.16.3.252 172.16.3.253
```

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

# origin

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

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

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

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

**Defaults** The default size value is /0.

**Command Modes** DHCP pool configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.3(11)T	The <b>file</b> keyword was added.

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

Use the **dhcp** keyword to obtain subnets from DHCP, the **aaa** keyword to obtain subnets from the AAA server, and the **ipcp** keyword to obtain subnets from IPCP negotiation. If you expect that the utilization of the pool may grow over time, use the **autogrow** *size* option. If a pool has been configured with the **autogrow** *size* option, ensure that the source server is capable of providing more than one subnet to the same pool. Even though the Cisco IOS software specifies the requested subnet size, it can accept any offered subnet size from the source server.

---

**Examples**

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

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

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

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

---

**Related Commands**

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

---

## password (DFP agent)

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

```
password [0 | 7] password [timeout]
```

```
no password
```

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

**Defaults** No password is enabled.

**Command Modes** DFP agent configuration

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

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

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

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

**Examples**

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

```
Router(config)# ip dfp agent slb
Router(config-dfp)# password Cookies 360
```

**Related Commands**

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

## permit (IP)

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

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

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

```
no sequence-number
```

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

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

### Internet Control Message Protocol (ICMP)

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

### Internet Group Management Protocol (IGMP)

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


### Transmission Control Protocol (TCP)

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

### User Datagram Protocol (UDP)

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

## Syntax Description

<i>sequence-number</i>	(Optional) Sequence number assigned to the permit statement. The sequence number causes the system to insert the statement in that numbered position in the access list.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> <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 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.
 <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>permit</b> command.
<b>icmp</b>	Permits 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>permit</b> command.
<b>igmp</b>	Permits 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>permit</b> command.
<b>tcp</b>	Permits 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>permit</b> command.
<b>udp</b>	Permits 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>permit</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>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination 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>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>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 3</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>permit</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 (IP extended)</b> 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 matches IP packets if their TCP headers contain the TCP flags that are specified by the <i>flag-name</i> argument. The - keyword matches IP packets that do not contain the TCP flags specified by the <i>flag-name</i> argument. You must follow the + and - keywords with the <i>flag-name</i> argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: <b>urg</b>, <b>ack</b>, <b>psh</b>, <b>rst</b>, <b>syn</b>, and <b>fin</b>.</p>

**Syntax Description**

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

**Command Modes**

Access list configuration

**Command History**

Release	Modification
11.2	This command was introduced.
12.0(1)T	The <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> , + and - keywords and the <i>flag-name</i> argument were added.
12.3(7)T	Command functionality was modified to allow up to ten port numbers to be added after the <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 define the conditions under which a packet passes the named access list.

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

**log Keyword**

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

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

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

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

**Access List Filtering of IP Options**

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from their URL: [www.iana.org](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 3](#).

**Table 3** IP Option Values and Names

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

### Filtering IP Packets Based on TCP Flags

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

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

### Access List Processing of Fragments

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

If the Access-List Entry Has...	Then...
...no <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:

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

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

```
time-range testing
 periodic Monday Tuesday Friday 9:00 to 17:00
!
ip access-list extended legal
 permit tcp any any eq telnet time-range testing
!
interface ethernet 0
 ip access-group legal in
```

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

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

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

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

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

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

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

```
Router# show access-lists

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

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

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

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

```
Router# show access-lists

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

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

```
Router# show access-lists 101

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

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

```
Router# show access-lists 101

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

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

```
Router# show access-lists 101

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

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

Duplicate sequence number.

Router(config-ext-nacl)# end

Router# show access-lists 101

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

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

```
Router# show access-lists aaa

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

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

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

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

```
Router# show access-lists aaa

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



## Related Commands

Command	Description
<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>deny (IP)</b>	Sets conditions under which a packet does not pass a named IP access list.
<b>ip access-group</b>	Controls access to an interface.
<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>periodic</b>	Specifies a recurring (weekly) time range for functions that support the time-range feature.
<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.

## port (DFP agent)

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

**port** *port-number*

**no port** *port-number*

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

<b>Defaults</b>	No port number is defined.
-----------------	----------------------------

<b>Command Modes</b>	DFP agent configuration
----------------------	-------------------------

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

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

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

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

# predictor

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

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

**no predictor**

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

**Defaults** The default predictor is weighted round robin.

**Command Modes** SLB server farm configuration

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

**Examples** The following example specifies the weighted least connections algorithm:

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

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

# real

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

**real** *ip-address*

**no real** *ip-address*

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

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	SLB server farm configuration
----------------------	-------------------------------

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

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

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

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

# reassign

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

**reassign** *threshold*

**no reassign**

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

<b>Defaults</b>	The default threshold is three SYNs.
-----------------	--------------------------------------

<b>Command Modes</b>	SLB real server configuration
----------------------	-------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(7)XE</td> <td>This command was introduced.</td> </tr> <tr> <td>12.1(5)T</td> <td>This command was integrated into Cisco IOS Release 12.1(5)T.</td> </tr> </tbody> </table>	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.
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.						

<b>Examples</b>	The following example sets the threshold of unanswered SYNs to 2:
-----------------	---

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

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>real</b></td> <td>Identifies a real server.</td> </tr> <tr> <td><b>show ip slb reals</b></td> <td>Displays information about the real servers.</td> </tr> <tr> <td><b>show ip slb serverfarms</b></td> <td>Displays information about the server farm configuration.</td> </tr> </tbody> </table>	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.
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.								

# relay agent information

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

**relay agent information**

**no relay agent information**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** DHCP class configuration

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

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

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

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

```
ip dhcp class CLASS1
  relay agent information
    relay-information hex 01030a0b0c020500000000123
    relay-information hex 01030a0b0c02*
    relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF

ip dhcp class CLASS2
  relay agent information
```

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

# relay-information hex

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

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

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

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

**Defaults** No default behavior or values

**Command Modes** Relay agent information option configuration mode.

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

**Usage Guidelines**

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

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

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

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

---

**Examples**

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

```
ip dhcp class CLASS1
  relay agent information
    relay-information hex 01030a0b0c020500000000123
    relay-information hex 01030a0b0c02*
    relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF

ip dhcp class CLASS2
  relay agent information
```



# release dhcp

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

**release dhcp** *type number*

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

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

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

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

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

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

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

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

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

Command	Description
<b>show running-config</b>	Displays the contents of the currently running configuration file or the configuration for a specific interface.
<b>show startup-config</b>	Displays the contents of the configuration file that will be used at the next system startup.

# remark

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

**remark** *remark*

**no remark** *remark*

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

<b>Defaults</b>	The access-list entries have no remarks.
-----------------	--

<b>Command Modes</b>	Standard named or extended named access list configuration
----------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(2)T	This command was introduced.

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

<b>Examples</b>	In the following example, the Jones subnet is not allowed to use outbound Telnet:
-----------------	---

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

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

## remote-ip (IPC transport-SCTP remote)

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

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

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

### Syntax Description

<i>peer-real-ip-address</i>	IP address of the remote peer.  The remote IP addresses must match the local IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global Virtual Routing and Forwarding (VRF). A virtual IP (VIP) address cannot be used.
<i>peer-real-ip-address2</i>	(Optional) IP address of the remote peer.

### Defaults

No IP addresses are defined.

### Command Modes

IPC transport-SCTP remote configuration

### Command History

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

### Usage Guidelines

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

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

### Examples

The following example shows how to enable SSO:

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

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

# remote-port

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

**remote-port** *remote-port-number*

<b>Syntax Description</b>	<i>remote-port-number</i>	Remote port number, which should be the same as the local port number on the peer router (which is specified via the <b>local-port</b> command).
---------------------------	---------------------------	--

**Defaults** A remote SCTP port is not defined.

**Command Modes** SCTP protocol configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(8)T	

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

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

```

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

```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	local-port	Defines the local SCTP port that is used to communicate with the redundant peer.
	remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.

# renew dhcp

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

**renew dhcp** *type number*

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

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

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

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

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

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

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

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

Related Commands	Command	Description
	<b>ip address dhcp</b>	Specifies that the Ethernet interface acquires an IP address through DHCP.
	<b>lease</b>	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.
	<b>release dhcp</b>	Releases the DHCP lease on the specified interface.
	<b>show dhcp lease</b>	Displays the DHCP addresses leased from a server.
	<b>show interface</b>	Displays statistics for all interfaces configured on the router or access server.
	<b>show ip dhcp binding</b>	Displays address bindings on the Cisco IOS DHCP server.
	<b>show ip interface</b>	Displays a summary of an interface's IP information and status.

Command	Description
<b>show running-config</b>	Displays the contents of the currently running configuration file or the configuration for a specific interface.
<b>show startup-config</b>	Displays the contents of the configuration file that will be used at the next system startup.



## retry (real server)

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

**retry** *retry-value*

**no** **retry**

<b>Syntax Description</b>	<p><i>retry-value</i></p> <p>Time, in seconds, to wait after the detection of a server failure before a new connection to the server is attempted.</p> <p>If the new connection attempt succeeds, the real server is placed in <b>OPERATIONAL</b> state. If the connection attempt fails, the timer is reset, the connection is reassigned, and the process repeats until it is successful or until the server is placed <b>OUTOFSERVICE</b> by the network administrator.</p> <p>Valid values range from 1 to 3600. The default value is 60 seconds.</p> <p>A value of 0 means do not attempt a new connection to the server when it fails.</p>
---------------------------	--

<b>Defaults</b>	The <i>retry-value</i> default is 60 seconds.
-----------------	---

<b>Command Modes</b>	SLB real server configuration
----------------------	-------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(7)XE</td> <td>This command was introduced.</td> </tr> <tr> <td>12.1(5)T</td> <td>This command was integrated into Cisco IOS Release 12.1(5)T.</td> </tr> </tbody> </table>	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.
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.						

<b>Examples</b>	<p>The following example specifies that 120 seconds must elapse after the detection of a server failure before a new connection is attempted:</p>
-----------------	---

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

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>real</b></td> <td>Identifies a real server.</td> </tr> <tr> <td><b>show ip slb reals</b></td> <td>Displays information about the real servers.</td> </tr> <tr> <td><b>show ip slb serverfarms</b></td> <td>Displays information about the server farm configuration.</td> </tr> </tbody> </table>	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.
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.								

# serverfarm

To associate a real server farm with a virtual server, use the **serverfarm** command in SLB virtual server configuration mode. To remove the server farm association from the virtual server configuration, use the **no** form of this command.

**serverfarm** *serverfarm-name*

**no serverfarm**

<b>Syntax Description</b>	<i>serverfarm-name</i>	Name of a server farm that has already been defined using the <b>ip slb serverfarm</b> command.
---------------------------	------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	SLB virtual server configuration
----------------------	----------------------------------

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

**Examples** The following example shows how the **ip slb vserver**, **virtual**, and **serverfarm** commands are used to associate the real server farm named PUBLIC with the virtual server named PUBLIC\_HTTP:

```
ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
serverfarm PUBLIC
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ip slb vservers</b>	Displays information about the virtual servers.
<b>virtual</b>	Configures the virtual server attributes.	

# service dhcp

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

**service dhcp**

**no service dhcp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Enabled

**Command Modes** Global configuration

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

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

**Examples** The following example enables DHCP services on the DHCP server:

```
service dhcp
```

# set ip next-hop dynamic dhcp

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

**set ip next-hop dynamic dhcp**

**no set ip next-hop dynamic dhcp**

**Syntax Description** This command has no arguments or keywords.

**Defaults** This command is disabled by default.

**Command Modes** Route-map configuration

Command History	Release	Modification
	12.3(2)XE	This command was introduced.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.

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

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

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

Related Commands	Command	Description
	<b>access list (IP extended)</b>	Defines an extended IP access list.

# show access-list compiled

To display a table showing Turbo Access Control Lists (ACLs), use the **show access-list compiled** command in EXEC mode.

## show access-list compiled

**Syntax Description** This command has no arguments or keywords.

**Command Modes**  
User EXEC  
Privileged EXEC

Command History	Release	Modification
	12.0(6)S	This command was introduced.
	12.1(1)E	This command was introduced for Cisco 7200 series routers.
	12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

**Usage Guidelines** This command is used to display the status and condition of the Turbo ACL tables associated with each access list. The memory usage is displayed for each table; large and complex access lists may require substantial amounts of memory. If the memory usage is greater than the memory available, you can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the access lists is not then enabled.

**Examples** The following is partial sample output from the **show access-list compiled** command:

```
Router# show access-list compiled

Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
ACL          State      Tables  Entries  Config  Fragment  Redundant  Memory
1            Operational  1        2        1        0          0          1Kb
2            Operational  1        3        2        0          0          1Kb
3            Operational  1        4        3        0          0          1Kb
4            Operational  1        3        2        0          0          1Kb
5            Operational  1        5        4        0          0          1Kb
9            Operational  1        3        2        0          0          1Kb
20           Operational  1        9        8        0          0          1Kb
21           Operational  1        5        4        0          0          1Kb
101          Operational  1        15       9        7          2          1Kb
102          Operational  1        13       6        6          0          1Kb
120          Operational  1        2        1        0          0          1Kb
199          Operational  1        4        3        0          0          1Kb
First level lookup tables:
Block      Use              Rows      Columns  Memory used
0          TOS/Protocol     6/16     12/16    66048
1          IP Source (MS)   10/16    12/16    66048
2          IP Source (LS)   27/32    12/16    132096
```

3	IP Dest (MS)	3/16	12/16	66048
4	IP Dest (LS)	9/16	12/16	66048
5	TCP/UDP Src Port	1/16	12/16	66048
6	TCP/UDP Dest Port	3/16	12/16	66048
7	TCP Flags/Fragment	3/16	12/16	66048

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>access-list compiled</b>	Enables the Turbo ACL feature.
<b>access-list (extended)</b>	Provides extended access lists that allow more detailed access lists.
<b>access-list (standard)</b>	Creates a standard access list.
<b>clear access-list counters</b>	Clears the counters of an access list.
<b>clear access-temp</b>	Manually clears a temporary access list entry from a dynamic access list.
<b>ip access-list</b>	Defines an IP access list by name.
<b>show ip access-list</b>	Displays the contents of all current IP access lists.

# show access-lists

To display the contents of current access lists, use the **show access-lists** command in privileged EXEC mode.

```
show access-lists [access-list-number | access-list-name]
```

Syntax Description		
	<i>access-list-number</i>	(Optional) Number of the access list to display. The system displays all access lists by default.
	<i>access-list-name</i>	(Optional) Name of the IP access list to display.

**Defaults** The system displays all access lists.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(5)T	The command output was modified to identify compiled access lists.
	12.2(2)T	The command output was modified to show information for IPv6 access lists.

**Examples** The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101

Extended IP access list 101
  permit tcp host 198.92.32.130 any established (4304 matches) check=5
  permit udp host 198.92.32.130 any eq domain (129 matches)
  permit icmp host 198.92.32.130 any
  permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
  permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
  permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
  permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
  permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
  permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
  deny ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
  deny ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
  deny ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
  deny ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
  deny ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
  deny ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the **show access-lists** command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

**Note**

The permit and deny information displayed by the **show access-lists** command may not be in the same order as that entered using the **access-list** command

```
Router# show access-lists
Standard IP access list 1 (Compiled)
  deny any
Standard IP access list 2 (Compiled)
  deny 192.168.0.0, wildcard bits 0.0.0.255
  permit any
Standard IP access list 3 (Compiled)
  deny 0.0.0.0
  deny 192.168.0.1, wildcard bits 0.0.0.255
  permit any
Standard IP access list 4 (Compiled)
  permit 0.0.0.0
  permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists

IPv6 access list list2
  deny ipv6 FEC0:0:0:2::/64 any sequence 10
  permit ipv6 any any sequence 20
```

For information on how to configure access lists, refer to the “Configuring IP Services” chapter of the *Cisco IOS IP Configuration Guide*.

For information on how to configure dynamic access lists, refer to the “Traffic Filtering and Firewalls” part of the *Cisco IOS Security Configuration Guide*.

**Related Commands**

Command	Description
<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>clear access-list counters</b>	Clears the counters of an access list.
<b>clear access-template</b>	Clears a temporary access list entry from a dynamic access list manually.
<b>ip access-list</b>	Defines an IP access list by name.
<b>show ip access-lists</b>	Displays the contents of all current IP access lists.
<b>show ipv6 access-list</b>	Displays the contents of all current IPv6 access lists.



# show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** privileged EXEC command.

**show arp**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

**Examples** The following is sample output from the **show arp** command:

Router# **show arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	131.108.42.112	120	0000.a710.4baf	ARPA	Ethernet3
AppleTalk	4028.5	29	0000.0c01.0e56	SNAP	Ethernet2
Internet	131.108.42.114	105	0000.a710.859b	ARPA	Ethernet3
AppleTalk	4028.9	-	0000.0c02.a03c	SNAP	Ethernet2
Internet	131.108.42.121	42	0000.a710.68cd	ARPA	Ethernet3
Internet	131.108.36.9	-	0000.3080.6fd4	SNAP	TokenRing0
AppleTalk	4036.9	-	0000.3080.6fd4	SNAP	TokenRing0
Internet	131.108.33.9	-	0000.0c01.7bbd	SNAP	Fddi0

[Table 4](#) describes the significant fields shown in the display.

**Table 4** *show arp* Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

**Table 4** *show arp Field Descriptions (continued)*

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: <ul style="list-style-type: none"><li>• ARPA</li><li>• SNAP</li><li>• ETLK (EtherTalk)</li><li>• SMDS</li></ul>
Interface	Indicates the interface associated with this network address.

# show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

```
show glbp [interface-type interface-number] [group-number] [state] [brief]
```

Syntax Description	
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number for which output is displayed.
<i>group-number</i>	(Optional) GLBP group number in the range from 0 to 1023.
<i>state</i>	(Optional) State of the GLBP router, one of the following: <b>active</b> , <b>disabled</b> , <b>init</b> , <b>listen</b> , <b>speak</b> , and <b>standby</b> .
<b>brief</b>	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.

Command Modes	
	Privileged EXEC

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 output was enhanced to display information about Message Digest 5 (MD5) authentication.
	12.3(7)T	The output was enhanced to display information about assigned redundancy names to specified groups.

Usage Guidelines	
	Use the <b>show glbp</b> command to display information about GLBP groups on a router. The <b>brief</b> keyword displays a single line of information about each virtual gateway or virtual forwarder.

Examples	
	The following is sample output from the <b>show glbp</b> command:

```
Router# show glbp

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication MD5, key "ThisStringIsTheSecretKey"
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
  Track object 2 state Down decrement 5
```

```

Load balancing: host-dependent
There is 1 forwarder (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 23:50:15
  MAC address is 0007.b400.0101 (default)
  Owner ID is 0005.0050.6c08
  Redirection enabled
  Preemption enabled, min delay 60 sec
  Active is local, weighting 105

```

The following is sample output from the **show glbp** command with the **brief** keyword specified:

```
Router# show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Fa0/0	10	-	254	Active	10.21.8.10	local	unknown
Fa0/0	10	1	7	Active	0007.b400.0101	local	-

The following is sample output from the **show glbp** command that displays GLBP group 10:

```
Router# show glbp 10
```

```

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
  Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication MD5, key "ThisStringIsTheSecretKey"
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
  Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
    Redirection enabled
    Preemption enabled, min delay 60 sec
    Active is local, weighting 105

```

The following is sample output from the **show glbp** command with the **brief** keyword specified:

```
Router# show glbp brief
```

Interface	Grp	Fwd	Pri	State	Address	Active router	Standby router
Fa0/0	10	-	254	Active	10.21.8.10	local	unknown
Fa0/0	10	1	7	Active	0007.b400.0101	local	-

The following output shows that the redundancy name has been assigned to the “glbp1” group:

```
Router# show glbp ethernet0/1 1

Ethernet0/1 - Group 1
  State is Listen
    64 state changes, last state change 00:00:54
  Virtual IP address is 10.1.0.7
  Hello time 50 msec, hold time 200 msec
    Next hello sent in 0.030 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Authentication text "authword"
  Preemption enabled, min delay 0 sec
  Active is 10.1.0.2, priority 105 (expires in 0.184 sec)
  Standby is 10.1.0.3, priority 100 (expires in 0.176 sec)
  Priority 96 (configured)
  Weighting 100 (configured 100), thresholds: lower 95, upper 100
    Track object 1 state Up decrement 10
  Load balancing: round-robin
  IP redundancy name is "glbp1"
  Group members:
    0004.4d83.4801 (10.0.0.0)
    0010.7b5a.fa41 (10.0.0.1)
    00d0.bb33.bc21 (10.0.0.2) local
```

Table 5 describes the significant fields shown in the displays.

**Table 5** *show glbp Field Descriptions*

Field	Description
FastEthernet0/0 - Group	Interface type and number and GLBP group number for the interface.
State is	<p>State of the virtual gateway or virtual forwarder. For a virtual gateway, the state can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Active</b>—The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address.</li> <li>• <b>Disabled</b>—The virtual IP address has not been configured or learned yet, but another GLBP configuration exists.</li> <li>• <b>Initial</b>—The virtual IP address has been configured or learned, but virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured.</li> <li>• <b>Listen</b>—The virtual gateway is receiving hello packets and is ready to change to the “speak” state if the active or standby virtual gateway becomes unavailable.</li> <li>• <b>Speak</b>—The virtual gateway is attempting to become the active or standby virtual gateway.</li> <li>• <b>Standby</b>—The gateway is next in line to be the AVG.</li> </ul>

Table 5 *show glbp Field Descriptions (continued)*

Field	Description
	<p>For a virtual forwarder, the state can be one of the following:</p> <ul style="list-style-type: none"> <li>• Active—The gateway is the active virtual forwarder (AVF) and is responsible for forwarding packets sent to the virtual forwarder MAC address.</li> <li>• Disabled—The virtual MAC address has not been assigned or learned. This is a transitory state because a virtual forwarder changing to a disabled state is deleted.</li> <li>• Initial—The virtual MAC address is known, but virtual forwarder configuration is not complete. An interface must be up and configured to route IP, an interface IP address must be configured, and the virtual IP address must be known.</li> <li>• Listen—The virtual forwarder is receiving hello packets and is ready to change to the “active” state if the AVF becomes unavailable.</li> </ul>
Virtual IP address is	The virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the router has failed to defend its ARP cache entry.
Hello time, hold time	The hello time is the time between hello packets (in seconds or milliseconds). The hold time is the time (in seconds or milliseconds) before other routers declare the active router to be down. All routers in a GLBP group use the hello- and hold-time values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello- and hold-time values.
Next hello sent in	The time until GLBP will send the next hello packet (in seconds or milliseconds).
Preemption	<p>Whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time (in seconds) for which a higher-priority nonactive router will wait before preempting the lower-priority active router.</p> <p>This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.</p>
Active is	<p>The active state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the current AVG.</p> <p>This field is also displayed under the forwarder section where it indicates the address of the current AVF.</p>
Standby is	The standby state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the standby gateway (the gateway that is next in line to be the AVG).
Weighting	The initial weighting value with lower and upper threshold values.
Track object	The list of objects that are being tracked and their corresponding states.
IP redundancy name is	The name of the GLBP group.

**show glbp****Related Commands**

<b>Command</b>	<b>Description</b>
<b>glbp ip</b>	Enables GLBP.
<b>glbp timers</b>	Configures the time between hello messages and the time before other routers declare the active GLBP router to be down.
<b>glbp weighting track</b>	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

# show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses, use the **show hosts** command in EXEC mode.

## show hosts

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(4)T	This command was updated to support the Cisco modem user interface feature.

**Examples** The following is sample output from the **show hosts** command:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host          Flag      Age    Type    Address(es)
SLAG.CISCO.COM (temp, OK) 1      IP      172.20.4.10
CHAR.CISCO.COM (temp, OK) 8      IP      192.168.7.50
CHAOS.CISCO.COM (temp, OK) 8      IP      172.20.1.115
DIRT.CISCO.COM (temp, EX) 8      IP      172.20.1.111
DUSTBIN.CISCO.COM (temp, EX) 0      IP      172.20.1.27
DREGS.CISCO.COM (temp, EX) 24     IP      172.20.1.30
```

[Table 6](#) describes the significant fields shown in the display.

**Table 6** *show hosts Field Descriptions*

Field	Description
Flag	A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity.  A permanent entry is entered by a configuration command and is not timed out. Entries marked OK are believed to be valid. Entries marked ?? are considered suspect and subject to revalidation. Entries marked EX are expired.
Age	Indicates the number of hours since the software last referred to the cache entry.
Type	Identifies the type of address, for example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the <b>ip hp-host</b> global configuration command, the <b>show hosts</b> command will display these host names as type HP-IP.
Address(es)	Displays the address of the host. One host may have up to eight addresses.



The following is sample output from a router when a modem telephone number is mapped to an IP host address for the Cisco modem user interface feature using the **ip host** global configuration command:

```
Router# show hosts

Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Codes: u - unknown, e - expired, * - OK, ? - revalidate
       t - temporary, p - permanent

      Host                Age  Type    Address(es)
*p p4085554567           0   IP      1.2.1.6
*p t4085551234           0   IP      1.2.1.5
```

Under the Host field, a “p” preceding the number indicates a pulse-dialed modem telephone number, and a “t” indicates a tone-dialed modem telephone number. The IP address mapped to the telephone number appears under the Address(es) field. See [Table 6](#) for descriptions of the other fields seen in this display.

#### Related Commands

Command	Description
<b>clear arp interface</b>	Deletes entries from the host name-to-address cache.
<b>ip helper-address</b>	Defines a static host-name-to-address mapping in the host cache.

# show interface mac

To display MAC accounting information for interfaces configured for MAC accounting, use the **show interface mac** command in user EXEC or privileged EXEC mode.

**show interface** [*interface interface*] **mac**

<b>Syntax Description</b>	<i>type</i>	(Optional) Interface type supported on your router.
	<i>number</i>	(Optional) Port number of the interface. The syntax varies depending on the type router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash marks are required). Refer to the appropriate hardware manual for numbering information.
<b>Command Modes</b>	User EXEC Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1 CC	This command was introduced.

**Usage Guidelines** The **show interface mac** command displays information for all interfaces configured for MAC accounting. To display information for a single interface, use the **show interface type number mac** command.

For incoming packets on the interface, the accounting statistics are gathered before the CAR/DCAR feature is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after output CAR, before output DCAR or DWRED or DWFQ feature is performed on the packet. Therefore, if you are using DCAR or DWRED on the interface and packets are dropped, the dropped packets are still counted in the **show interface mac** command because the calculations are done prior to the features.

The maximum number of MAC addresses that can be stored for the input address is 512 and the maximum number of MAC address that can be stored for the output address is 512. After the maximum is reached, subsequent MAC addresses are ignored.

To clear the accounting statistics, use the **clear counter EXEC** command. To configure an interface for IP accounting based on the MAC address, use the **ip accounting mac-address** interface configuration command.

## Examples

The following is sample output from the **show interface mac** command. This feature calculates the total packet and byte counts for the interface that receives (input) or sends (output) IP packets to or from a unique MAC address. It also records a time stamp for the last packet received or sent.

```
Router# show interface ethernet 0/1/1 mac

Ethernet0/1/1
  Input (511 free)
```

## ■ show interface mac

```
0007.f618.4449(228): 4 packets, 456 bytes, last: 2684ms ago
                    Total: 4 packets, 456 bytes
Output (511 free)
0007.f618.4449(228): 4 packets, 456 bytes, last: 2692ms ago
                    Total: 4 packets, 456 bytes
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip accounting</b>	Enables IP accounting on any interface based on the source and destination
<b>mac-address</b>	MAC address.

---

# show interface precedence

To display precedence accounting information for interfaces configured for precedence accounting, use the **show interface precedence** command in user EXEC or privileged EXEC mode.

**show interface** [*type number*] **precedence**

Syntax Description	<i>type</i>	(Optional) Interface type supported on your router.
	<i>number</i>	(Optional) Port number of the interface. The syntax varies depending on the type router. For example, on a Cisco 7500 series router the syntax is 0/0/0, where 0 represents the slot, port adapter, and port number (the slash is required). Refer to the appropriate hardware manual for numbering information.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines	<p>The <b>show interface precedence</b> command displays information for all interfaces configured for IP precedence accounting. To display information for a single interface, use the <b>show interface <i>type number</i> precedence</b> command.</p> <p>For incoming packets on the interface, the accounting statistics are gathered before input CAR/DCAR is performed on the packet. Therefore, if CAR/DCAR changes the precedence on the packet, it is counted based on the old precedence setting with the <b>show interface precedence</b> command.</p> <p>For outgoing packets on the interface, the accounting statistics are gathered after output DCAR or DWRED or DWFQ feature is performed on the packet.</p> <p>To clear the accounting statistics, use the <b>clear counter</b> EXEC command.</p> <p>To configure an interface for IP accounting based on IP precedence, use the <b>ip accounting precedence</b> interface configuration command.</p>
------------------	---

Examples	<p>The following is sample output from the <b>show interface precedence</b> command. This feature calculates the total packet and byte counts for the interface that receives (input) or sends (output) IP packets and sorts the results based on IP precedence.</p>
----------	--

```
Router# show interface ethernet 0/1/1 precedence
Ethernet0/1/1
  Input
    Precedence 0:  4 packets, 456 bytes
  Output
    Precedence 0:  4 packets, 456 bytes
```

■ show interface precedence

---

**Related Commands**

Command	Description
<b>ip accounting precedence</b>	Enables IP accounting on any interface based on IP precedence.

---

# show ip access-list

To display the contents of all current IP access lists, use the **show ip access-list** command in user EXEC or privileged EXEC mode.

**show ip access-list** [*access-list-number* | *access-list-name* / **dynamic** *access-list-name*]

Syntax Description	
<i>access-list-number</i>	(Optional) Number of the IP access list to display.
<i>access-list-name</i>	(Optional) Name of the IP access list to display.
<b>dynamic</b>	(Optional) Lists dynamic IP access lists.

**Defaults** All standard and extended IP access lists are displayed.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.3(7)T	The <b>dynamic</b> keyword was added.

**Usage Guidelines** The **show ip access-list** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

**Examples** The following is sample output from the **show ip access-list** command when all access lists are requested:

```
Router# show ip access-list

Extended IP access list 101
  deny udp any any eq ntp
  permit tcp any any
  permit udp any any eq tftp
  permit icmp any any
  permit udp any any eq domain
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Router# show ip access-list Internetfilter

Extended IP access list Internetfilter
  permit tcp any 172.31.0.0 0.0.255.255 eq telnet
  deny tcp any any
  deny udp any 172.31.0.0 0.0.255.255 lt 1024
  deny ip any any log
```

# show ip accounting

To display the active accounting or checkpointed database or to display access list violations, use the **show ip accounting** command in user EXEC or privileged EXEC mode.

**show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]

Syntax Description	Parameter	Description
	<b>checkpoint</b>	(Optional) Indicates that the checkpointed database should be displayed.
	<b>output-packets</b>	(Optional) Indicates that information pertaining to packets that passed access control and were routed should be displayed. If neither the <b>output-packets</b> nor <b>access-violations</b> keyword is specified, <b>output-packets</b> is the default.
	<b>access-violations</b>	(Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. If neither the <b>output-packets</b> nor <b>access-violations</b> keyword is specified, <b>output-packets</b> is the default.

## Defaults

If neither the **output-packets** nor **access-violations** keyword is specified, the **show ip accounting** command displays information pertaining to packets that passed access control and were routed.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
10.0	This command was introduced.
10.3	The <b>output-packets</b> and <b>access-violations</b> keywords were added.

## Usage Guidelines

If you do not specify any keywords, the **show ip accounting** command displays information about the active accounting database.

To display IP access violations, you must use the **access-violations** keyword. If you do not specify the keyword, the command defaults to displaying the number of packets that have passed access lists and were routed.

To use this command, you must first enable IP accounting on a per-interface basis.

## Examples

The following is sample output from the **show ip accounting** command:

```
Router# show ip accounting
```

Source	Destination	Packets	Bytes
131.108.19.40	192.67.67.20	7	306
131.108.13.55	192.67.67.20	67	2749
131.108.2.50	192.12.33.51	17	1111
131.108.2.50	130.93.2.1	5	319
131.108.2.50	130.93.1.2	463	30991

```

131.108.19.40    130.93.2.1          4          262
131.108.19.40    130.93.1.2         28         2552
131.108.20.2     128.18.6.100      39         2184
131.108.13.55    130.93.1.2         35         3020
131.108.19.40    192.12.33.51      1986       95091
131.108.2.50     192.67.67.20      233        14908
131.108.13.28    192.67.67.53      390        24817
131.108.13.55    192.12.33.51     214669     9806659
131.108.13.111   128.18.6.23       27739     1126607
131.108.13.44    192.12.33.51     35412     1523980
192.31.7.21      130.93.1.2         11         824
131.108.13.28    192.12.33.2        21         1762
131.108.2.166    192.31.7.130      797        141054
131.108.3.11     192.67.67.53       4          246
192.31.7.21      192.12.33.51     15696     695635
192.31.7.24      192.67.67.20      21         916
131.108.13.111   128.18.10.1        16         1137
accounting threshold exceeded for 7 packets and 433 bytes

```

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

```
Router# show ip accounting access-violations
```

```

      Source          Destination      Packets      Bytes      ACL
131.108.19.40      192.67.67.20         7          306        77
131.108.13.55      192.67.67.20        67         2749       185
131.108.2.50       192.12.33.51        17         1111       140
131.108.2.50       130.93.2.1           5          319        140
131.108.19.40      130.93.2.1           4          262         77
Accounting data age is 41

```

[Table 7](#) describes the significant fields shown in the displays.

**Table 7** *show ip accounting Field Descriptions*

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets sent from the source address to the destination address. With the <b>access-violations</b> keyword, the number of packets sent from the source address to the destination address that violated an access control list (ACL).
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets sent from the source address to the destination address. With the <b>access-violations</b> keyword, the total number of bytes sent from the source address to the destination address that violated an ACL.
ACL	Number of the access list of the last packet sent from the source to the destination that failed an access list filter.
accounting threshold exceeded...	Data for all packets that could not be entered into the accounting table when the accounting table is full. This data is combined into a single entry.



**show ip accounting****Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear ip accounting</b>	Clears the active or checkpointed database when IP accounting is enabled.
<b>ip accounting</b>	Enables IP accounting on an interface.
<b>ip accounting-list</b>	Defines filters to control the hosts for which IP accounting information is kept.
<b>ip accounting-threshold</b>	Sets the maximum number of accounting entries to be created.
<b>ip accounting-transits</b>	Controls the number of transit records that are stored in the IP accounting database.

# show ip aliases

To display the IP addresses mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similarly to aliases, use the **show ip aliases** EXEC command.

## show ip aliases

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** To distinguish a SLIP address from a normal alias address, the command output uses the form SLIP TTY1 for the “port” number, where 1 is the auxiliary port.

**Examples** The following is sample output from the **show ip aliases** command:

```
Router# show ip aliases

  IP Address   Port
131.108.29.245 SLIP TTY1
```

The display lists the IP address and corresponding port number.

Related Commands	Command	Description
	<b>show line</b>	Displays the parameters of a terminal line.

# show ip arp

To display the Address Resolution Protocol (ARP) cache, where Serial Line Internet Protocol (SLIP) addresses appear as permanent ARP table entries, use the **show ip arp** EXEC command.

```
show ip arp [ip-address] [host-name] [mac-address] [interface type number]
```

Syntax Description	
<i>ip-address</i>	(Optional) ARP entries matching this IP address are displayed.
<i>host-name</i>	(Optional) Host name.
<i>mac-address</i>	(Optional) 48-bit MAC address.
<i>interface type number</i>	(Optional) ARP entries learned via this interface type and number are displayed.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	9.0	This command was introduced.

**Usage Guidelines** ARP establishes correspondences between network addresses (an IP address, for example) and LAN hardware addresses (Ethernet addresses). A record of each correspondence is kept in a cache for a predetermined amount of time and then discarded.

**Examples** The following is sample output from the **show ip arp** command:

```
Router# show ip arp

Protocol  AddressAge(min)  Hardware Addr  Type   Interface
Internet  171.69.233.2290000.0c59.f892  ARPA    Ethernet0/0
Internet  171.69.233.2180000.0c07.ac00  ARPA    Ethernet0/0
Internet  171.69.233.19-0000.0c63.1300  ARPA    Ethernet0/0
Internet  171.69.233.3090000.0c36.6965  ARPA    Ethernet0/0
Internet  172.19.168.11-0000.0c63.1300  ARPA    Ethernet0/0
Internet  172.19.168.25490000.0c36.6965  ARPA    Ethernet0/0
```

[Table 8](#) describes the significant fields shown in the display.

**Table 8** *show ip arp* Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

**Table 8** *show ip arp Field Descriptions (continued)*

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using the network address in this entry. Possible value include: <ul style="list-style-type: none"><li>• ARPA</li><li>• SNAP</li><li>• SAP</li></ul>
Interface	Indicates the interface associated with this network address.

# show ip casa affinities

To display statistics about affinities, use the **show ip casa affinities** command in user EXEC or privileged EXEC mode.

```
show ip casa affinities [stats] | [saddr ip-address [detail]] | [daddr ip-address [detail]] | sport
source-port [detail] | dport destination-port [detail] | protocol protocol [detail]
```

Syntax Description		
<b>stats</b>	(Optional)	Displays limited statistics.
<b>saddr</b> <i>ip-address</i>	(Optional)	Displays the source address of a given TCP connection.
<b>detail</b>	(Optional)	Displays the detailed statistics.
<b>daddr</b> <i>ip-address</i>	(Optional)	Displays the destination address of a given TCP connection.
<b>sport</b> <i>source-port</i>	(Optional)	Displays the source port of a given TCP connection.
<b>dport</b> <i>destination-port</i>	(Optional)	Displays the destination port of a given TCP connection.
<b>protocol</b> <i>protocol</i>	(Optional)	Displays the protocol of a given TCP connection.

Command Modes	
	User EXEC
	Privileged EXEC

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

## Examples

The following is sample output of the **show ip casa affinities** command:

```
Router# show ip casa affinities

                          Affinity Table
Source Address  Port  Dest Address  Port  Prot
161.44.36.118  1118  172.26.56.13  19    TCP
172.26.56.13   19    161.44.36.118  1118  TCP
```

The following is sample output of the **show ip casa affinities detail** command:

```
Router# show ip casa affinities detail

                          Affinity Table
Source Address  Port  Dest Address  Port  Prot
161.44.36.118  1118  172.26.56.13  19    TCP
Action Details:
  Interest Addr:          172.26.56.19      Interest Port: 1638
  Interest Packet: 0x0102 SYN FRAG
  Interest Tickle: 0x0005 FIN RST
  Dispatch (Layer 2):    YES              Dispatch Address: 172.26.56.33

Source Address  Port  Dest Address  Port  Prot
172.26.56.13   19    161.44.36.118  1118  TCP
Action Details:
  Interest Addr:          172.26.56.19      Interest Port: 1638
  Interest Packet: 0x0104 RST FRAG
```

```
Interest Tickle: 0x0003 FIN SYN
Dispatch (Layer 2): NO           Dispatch Address: 0.0.0.0
```

Table 9 describes the significant fields shown in the display.

**Table 9** *show ip casa affinities Field Descriptions*

Field	Description
Source Address	Source address of a given TCP connection.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Port	Destination of a given TCP connection.
Prot	Protocol of a given TCP connection.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager address that is to receive interest packets for this affinity.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of TCP packet types of interest to the services manager is interested in.
Interest Tickle	List of TCP packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.

#### Related Commands

Command	Description
<b>forwarding-agent</b>	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.
<b>show ip casa oper</b>	Displays operational information about the forwarding agent.

# show ip casa oper

To display operational information about the forwarding agent, use the **show ip casa oper** command in user EXEC or privileged EXEC mode.

**show ip casa oper**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

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

**Examples** The following is sample output from the **show ip casa oper** command:

```
Router# show ip casa oper

Casa is Active
  Casa control address is 206.10.20.34/32
  Casa multicast address is 224.0.1.2
  Listening for wildcards on:
    Port:1637
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:180 sec (Default)
```

[Table 10](#) describes the significant fields shown in the display.

**Table 10** *show ip casa oper Field Descriptions*

Field	Description
Casa is Active	The forwarding agent is active.
Casa control address	Unique address for this forwarding agent.
Casa multicast address	Services manager broadcast address.
Listening for wildcards on	Port on which the forwarding agent will listen.
Port	Services manager broadcast port.
Current passwd	Current password.
Pending passwd	Password that will override the current password.
Passwd timeout	Interval after which the pending password becomes the current password.

Related Commands	Command	Description
	<b>ip casa oper</b>	Configures the router to function as an MNLB forwarding agent.

# show ip casa stats

To display statistical information about the Forwarding Agent, use the **show ip casa stats** command in user EXEC or privileged EXEC mode.

## show ip casa stats

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

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

**Examples** The following is sample output of the **show ip casa stats** command:

```
Router# show ip casa stats

Casa is active:
  Wildcard Stats:
    Wildcards:          6           Max Wildcards:    6
    Wildcard Denies:    0           Wildcard Drops:   0
    Pkts Throughput:   441         Bytes Throughput: 39120
  Affinity Stats:
    Affinities:        2           Max Affinities:   2
    Cache Hits:        444         Cache Misses:     0
    Affinity Drops:    0
  Casa Stats:
    Int Packet:        4           Int Tickle:       0
    Casa Denies:       0           Drop Count:       0
```

[Table 11](#) describes the significant fields shown in the display.

**Table 11** *show ip casa stats Field Descriptions*

Field	Description
Casa is Active	The Forwarding Agent is active.
Wildcard Stats	Wildcard statistics.
Wildcards	Number of current wildcards.
Max Wildcards	Maximum number of wildcards since the Forwarding Agent became active.
Wildcard Denies	Protocol violations.
Wildcard Drops	Not enough memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.
Bytes Throughput	Number of bytes passed through all wildcards.



**Table 11** *show ip casa stats Field Descriptions (continued)*

Field	Description
Affinity Stats	Affinity statistics.
Affinities	Current number of affinities.
Max Affinities	Maximum number of affinities since the forwarding agent became active.
Cache Hits	Number of packets that match wildcards and fixed affinities.
Cache Misses	Matched wildcard, missed fix.
Affinity Drops	Number of times an affinity could not be created.
Casa Stats	Forwarding agent statistics.
Int Packet	Interest packets.
Int Tickle	Interest tickles.
Casa Denies	Protocol violation.
Security Drops	Packets dropped due to password or authentication mismatch.
Drop Count	Number of messages dropped.

**Related Commands**

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

# show ip casa wildcard

To display information about wildcard blocks, use the **show ip casa wildcard** command in user EXEC or privileged EXEC mode.

## show ip casa wildcard [detail]

<b>Syntax Description</b>	<b>detail</b>	(Optional) Displays detailed statistics.
<b>Command Modes</b>	User EXEC Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)T	This command was introduced.

## Examples

The following is sample output from the **show ip casa wildcard** command:

```
Router# show ip casa wildcard
```

Source Address	Source Mask	Port	Dest Address	Dest Mask	Port	Prot
0.0.0.0	0.0.0.0	0	172.26.56.2	255.255.255.255	0	ICMP
0.0.0.0	0.0.0.0	0	172.26.56.2	255.255.255.255	0	TCP
0.0.0.0	0.0.0.0	0	172.26.56.13	255.255.255.255	0	ICMP
0.0.0.0	0.0.0.0	0	172.26.56.13	255.255.255.255	0	TCP
172.26.56.2	255.255.255.255	0	0.0.0.0	0.0.0.0	0	TCP
172.26.56.13	255.255.255.255	0	0.0.0.0	0.0.0.0	0	TCP

The following is sample output from the **show ip casa wildcard detail** command:

```
router# show ip casa wildcard detail
```

Source Address	Source Mask	Port	Dest Address	Dest Mask	Port	Prot
0.0.0.0	0.0.0.0	0	172.26.56.2	255.255.255.255	0	ICMP

Service Manager Details:

Manager Addr: 172.26.56.19 Insert Time: 08:21:27 UTC 04/18/96

Affinity Statistics:

Affinity Count: 0 Interest Packet Timeouts: 0

Packet Statistics:

Packets: 0 Bytes: 0

Action Details:

Interest Addr: 172.26.56.19 Interest Port: 1638

Interest Packet: 0x8000 ALLPKTS

Interest Tickle: 0x0107 FIN SYN RST FRAG

Dispatch (Layer 2): NO Dispatch Address: 0.0.0.0

Advertise Dest Address: YES Match Fragments: NO

Source Address	Source Mask	Port	Dest Address	Dest Mask	Port	Prot
0.0.0.0	0.0.0.0	0	172.26.56.2	255.255.255.255	0	TCP

Service Manager Details:

Manager Addr: 172.26.56.19 Insert Time: 08:21:27 UTC 04/18/96

Affinity Statistics:

Affinity Count: 0 Interest Packet Timeouts: 0

Packet Statistics:

```

Packets:                0                Bytes: 0
Action Details:
Interest Addr:          172.26.56.19       Interest Port: 1638
Interest Packet: 0x8102 SYN FRAG ALLPKTS
Interest Tickle: 0x0005 FIN RST
Dispatch (Layer 2):    NO                Dispatch Address: 0.0.0.0
Advertise Dest Address: YES              Match Fragments: NO

```

**Note**

If a filter is not set, the filter is not active.

Table 12 describes significant fields shown in the display.

**Table 12** *show ip casa wildcard Field Descriptions*

Field	Description
Source Address	Source address of a given TCP connection.
Source Mask	Mask to apply to source address before matching.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Dest Mask	Mask to apply to destination address before matching.
Port	Destination port of a given TCP connection.
Prot	Protocol of a given TCP connection.
Service Manager Details	Services manager details.
Manager Addr	Source address of this wildcard.
Insert Time	System time at which this wildcard was inserted.
Affinity Statistics	Affinity statistics.
Affinity Count	Number of affinities created on behalf of this wildcard.
Interest Packet Timeouts	Number of unanswered interest packets.
Packet Statistics	Packet statistics.
Packets	Number of packets that match this wildcard.
Bytes	Number of bytes that match this wildcard.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.
Interest Tickle	List of packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.
Advertise Dest Address	Destination address.
Match Fragments	Does wildcard also match fragments? (boolean)

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

# show ip dfp

To display information about Dynamic Feedback Protocol (DFP) agents and their subsystems, use the **show ip dfp** command in privileged EXEC mode.

**show ip dfp** [*agent subsystem-name*] [**detail**]

Syntax Description	<b>agent</b> <i>subsystem-name</i>	(Optional) DFP agent information. The <i>subsystem-name</i> argument has a 15-character limit.
	<b>detail</b>	(Optional) Detailed DFP agent information.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Detailed output for the **show ip dfp** command includes information about all DFP agents configured with **ip slb agent** commands, regardless of whether those agents are currently in service.

**Examples** The following is sample output from the **show ip dfp** command:

```
Router# show ip dfp agent slb detail

Unexpected errors: 0

DFP Agent for service: SLB
  Port: 666 Interval: 10
  Current passwd: <none> Pending passwd: <none>
  Passwd timeout: 0
  Inservice: yes AppActive: yes

  Manager IP Address  Timeout
  -----
  172.18.45.27        0

Weight Table Report for Agent SLB

Weights for Port: 80 Protocol: TCP

  IP Address      Bind ID  Weight
  -----
  1.1.1.1         0       65535
```

```
Weights for Port: 0 (wildcard) Protocol: 0 (wildcard)
```

```
IP Address      Bind ID  Weight
-----
0.0.0.0         65534   0
```

```
Bind ID Table Report for Agent SLB
```

```
Bind IDs for Port: 80 Protocol: TCP
```

```
Bind ID  Client IP      Client Mask
-----
0         0.0.0.0         0.0.0.0
```

Table 13 describes the fields shown in the display.

**Table 13** *show ip dfp* Field Descriptions

Field	Description
Port	TCP port number of the agent.
Interval	Number of seconds to wait before recalculating weights.
Current passwd	Current DFP password for MD5 authentication.
Pending passwd	Pending new DFP password for MD5 authentication.
Passwd timeout	Delay period, in seconds, during which both the current password and the new password are accepted.
Inservice	DFP agent enabled for communication with a DFP manager.
AppActive	Active DFP agent.
Manager IP Address	IP address of the manager to which weights are being sent.
Timeout	Time period, in seconds, during which the DFP manager must receive an update from the DFP agent. A value of 0 means there is no timeout.
Weights for Port	Port for which the following weights are reported. 0 indicates a wildcard value.
Protocol	Protocol used for the port. 0 indicates a wildcard value.
IP Address	IP address for which weight is reported.
Bind ID	Bind ID associated with the IP address.
Weight	Weight calculated for the IP address.
Bind IDs for Port	Port for which the following bind IDs are reported.
Protocol	Protocol used for the port.
Bind ID	Bind ID of this instance of the real server.
Client IP	IP address of client using the virtual server.
Client Mask	IP network mask of client using the virtual server.

# show ip dhcp binding

Command	Description
<b>agent</b>	Identifies a DFP agent to which Cisco IOS SLB can connect.
<b>ip dfp agent</b>	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.
<b>ip slb dfp</b>	Configures DFP, supplies an optional password, and initiates DFP configuration mode.

To display address bindings on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp binding** command in user or privileged EXEC mode.

**show ip dhcp binding** [*ip-address*]

## Syntax Description

<i>ip-address</i>	(Optional) Specifies the IP address of the DHCP client for which bindings will be displayed.
-------------------	--

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(15)T	Support to display allocated subnets was added to the output.

## Usage Guidelines

This command is used to display DHCP binding information for IP address assignment and subnet allocation. If the address is not specified, all address bindings are shown. Otherwise, only the binding for the specified client is displayed. The output from this command displays binding information for individual IP address assignment and allocated subnets. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address only display an IP address and are not followed by a subnet mask.

## Examples

### IP Address Assignment Example

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, and the type of address assignment that have occurred. [Table 14](#) lists descriptions of the fields in each example.

```
Router# show ip dhcp binding 172.16.1.11
```

IP address	Hardware address	Lease expiration	Type
172.16.1.11	00a0.9802.32de	Feb 01 1998 12:00 AM	Automatic

```
Router# show ip dhcp binding 172.16.3.254
```

IP address	Hardware address	Lease expiration	Type
172.16.3.254	02c7.f800.0422	Infinite	Manual

**Table 14** *show ip dhcp binding Field Descriptions*

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

**Subnet Allocation Example**

The following example shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default). The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet) in CIDR bit count notation. Bindings for an individual IP address only display an IP address and are not followed by a subnet mask. [Table 15](#) lists descriptions of the fields in each example.

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

```
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration      Type
                Hardware address/
                User name
10.0.0.0/26     0063.6973.636f.2d64.   Mar 29 2003 04:36 AM   Automatic
                656d.6574.6572.2d47.
                4c4f.4241.4c
```

**Table 15** *show ip dhcp binding Field Descriptions*

Field	Description
IP address	The IP address of the host as recorded on the DHCP server. The subnet that follows the IP address (/26) in the example defines this binding as a subnet allocation binding.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date and time of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

**Related Commands**

Command	Description
<b>clear ip dhcp binding</b>	Deletes an automatic address binding from the Cisco IOS DHCP server database.



# show ip dhcp conflict

To display address conflicts found by a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server when addresses are offered to the client, use the **show ip dhcp conflict** command in user EXEC or privileged EXEC mode.

**show ip dhcp conflict** [*ip-address*]

<b>Syntax Description</b>	<i>ip-address</i> (Optional) Specifies the IP address of the conflict found.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(1)T	This command was introduced.

<b>Usage Guidelines</b>	The server uses ping to detect conflicts. The client uses gratuitous Address Resolution Protocol (ARP) to detect clients. If an address conflict is detected, the address is removed from the pool and the address is not assigned until an administrator resolves the conflict.
-------------------------	--

<b>Examples</b>	The following example displays the detection method and detection time for all IP addresses the DHCP server has offered that have conflicts with other devices. <a href="#">Table 16</a> lists descriptions of the fields in the example.
-----------------	---

```
Router# show ip dhcp conflict

IP address      Detection Method  Detection time
172.16.1.32     Ping              Feb 16 1998 12:28 PM
172.16.1.64     Gratuitous ARP    Feb 23 1998 08:12 AM
```

**Table 16** *show ip dhcp conflict Field Descriptions*

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP server. Can be a ping or a gratuitous ARP.
Detection time	The date and time when the conflict was found.

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear ip dhcp conflict</b>	Clears an address conflict from the Cisco IOS DHCP server database.

Command	Description
<b>ip dhcp ping packets</b>	Specifies the number of packets a Cisco IOS DHCP server sends to a pool address as part of a ping operation.
<b>ip dhcp ping timeout</b>	Specifies how long a Cisco IOS DHCP server waits for a ping reply from an address pool.

# show ip dhcp database

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database agent information, use the **show ip dhcp database** command in privileged EXEC mode.

**show ip dhcp database** [*url*]

## Syntax Description

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

## Defaults

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

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.0(1)T	This command was introduced.
12.3(1)T	The output was enhanced to display the text file that contains the static bindings.

## Examples

The following sample output shows that the text file was retrieved from the DHCP server:

```
Router# show ip dhcp database
URL      : ftp://myuserid:mypassword@10.0.0.0/staticbindingfile
Read     : Dec 01 2004 12:01 AM
Written  : Never
Status   : Last read succeeded. Bindings have been loaded in RAM.
Delay    : Not applicable
Timeout  : 300 seconds
Failures : 0
Successes : 1
```

The following sample output shows all DHCP server database agent information:

```
Router# show ip dhcp database

URL      :
ftp://user:password@172.16.4.253/router-dhcp
Read     : Dec 01 2004 12:01 AM
Written  : Never
Status   : Last read succeeded. Bindings have been loaded in RAM.
Delay    : 300 seconds
Timeout  : 300 seconds
Failures : 0
```

Successes : 1

Table 17 lists descriptions for each field in the samples.

**Table 17** *show ip dhcp database Field Descriptions*

Field	Description
URL	Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: <ul style="list-style-type: none"> <li>• tftp://host/filename</li> <li>• ftp://user:password@host/filename</li> <li>• rcp://user@host/filename</li> </ul>
Read	The last date and time bindings were read from the file server.
Written	The last date and time bindings were written to the file server.
Status	Indication of whether the last read or write of host bindings was successful.
Delay	The amount of time (in seconds) to wait before updating the database.
Timeout	The amount of time (in seconds) before the file transfer is aborted.
Failures	The number of failed file transfers.
Successes	The number of successful file transfers.

#### Related Commands

Command	Description
<b>ip dhcp database</b>	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.

# show ip dhcp import

To display the option parameters that were imported into the Dynamic Host Configuration Protocol (DHCP) server database, use the **show ip dhcp import** command in privileged EXEC command.

## show ip dhcp import

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.1(2)T	This command was introduced.

**Usage Guidelines** Imported option parameters are not part of the router configuration and are not saved in NVRAM. Thus, the **show ip dhcp import** command is necessary to display the imported option parameters.

**Examples** The following is sample output from the **show ip dhcp import** command:

```
Router# show ip dhcp import

Address Pool Name:2
Domain Name Server(s): 1.1.1.1
NetBIOS Name Server(s): 3.3.3.3
```

The following example indicates the address pool name:

```
Address Pool Name:2
```

The following example indicates the imported values, which are domain name and NetBIOS name information:

```
Domain Name Server(s): 1.1.1.1
NetBIOS Name Server(s): 3.3.3.3
```

Related Commands	Command	Description
	<b>import all</b>	Imports option parameters into the DHCP database.
	<b>show ip dhcp database</b>	Displays Cisco IOS server database information.

# show ip dhcp pool

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

**show ip dhcp pool** [*name*]

<b>Syntax Description</b>	<i>name</i>	(Optional) Displays information about a specific address pool. If not specified, displays information about all address pools.
---------------------------	-------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

<b>Usage Guidelines</b>	Use this command to determine the subnets allocated and to examine the current utilization level for the pool or all the pools if the <i>name</i> argument is not used.
-------------------------	---

**Examples** The following example shows DHCP address pool information for pool 1. [Table 18](#) lists descriptions for each field in the example.

```
Router# show ip dhcp pool 1

Pool 1:
Utilization mark (high/low)      : 85 / 15
Subnet size (first/next)         : 24 / 24 (autogrow)
VRF name                          : RED
Total addresses                  : 28
Leased addresses                 : 11
Pending event                    : none
2 subnets are currently in the pool :
Current index      IP address range      Leased addresses
10.1.1.12         10.1.1.1 - 10.1.1.14      11
10.1.1.17         10.1.1.17 - 10.1.1.30    0
```

**Table 18** *show ip dhcp pool* Field Descriptions

Field	Description
Pool 1	The name of the pool.
Utilization mark (high/low)	The configured high and low utilization level for the pool.
Subnet size (first/next)	The size of the requested subnets.
VRF name	The VRF name to which the pool is associated.
Total addresses	The total number of addresses in the pool.

**Table 18** *show ip dhcp pool Field Descriptions (continued)*

Field	Description
Leased addresses	The number of leased addresses in the pool.
Pending event	Displays any pending events.
2 subnets are currently in the pool	The number of subnets allocated to the address pool.
Current index	Displays the current index.
IP address range	The IP address range of the subnets.
Leased addresses	The number of leased addresses from each subnet.

# show ip dhcp relay information trusted-sources

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

## show ip dhcp relay information trusted-sources

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	12.2	This command was introduced.

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

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

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

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

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

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

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



# show ip dhcp server pool

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

**show ip dhcp server pool**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

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>host (host-list)</b>	Specifies a list of hosts that will receive 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>	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>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 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.

# show ip dhcp server statistics

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

## show ip dhcp server statistics

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

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

**Examples** The following example displays DHCP server statistics. [Table 19](#) lists descriptions for each field in the example.

```
Router> show ip dhcp server statistics
```

```
Memory usage          40392
Address pools         3
Database agents       1
Automatic bindings    190
Manual bindings       1
Expired bindings      3
Malformed messages    0
Secure arp entries    1

Message              Received
BOOTREQUEST          12
DHCPCDISCOVER        200
DHCPCREQUEST         178
DHCPCDECLINE         0
DHCPCRELEASE         0
DHCPCINFORM          0

Message              Sent
BOOTREPLY             12
DHCPOFFER            190
DHCPACK              172
DHCPCNAK              6
```

**Table 19** show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.

**Table 19** *show ip dhcp server statistics Field Descriptions (continued)*

Field	Description
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Secure arp entries	The number of ARP entries that have been secured to the MAC address of the client interface.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

**Related Commands**

Command	Description
<b>clear ip dhcp server statistics</b>	Resets all Cisco IOS DHCP server counters.

# show ip drp

To display information about the Director Response Protocol (DRP) Server Agent for DistributedDirector, use the **show ip drp** command in user EXEC or privileged EXEC mode.

## show ip drp

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	11.2 F	This command was introduced.

**Examples** The following is sample output from the **show ip drp** command:

```
Router# show ip drp
```

```
Director Responder Protocol Agent is enabled
717 director requests, 712 successful lookups, 5 failures, 0 no route
Authentication is enabled, using "test" key-chain
```

[Table 20](#) describes the significant fields shown in the display.

**Table 20** *show ip drp Field Descriptions*

Field	Description
director requests	Number of DRP requests that have been received (including any using authentication key-chain encryption that failed).
successful lookups	Number of successful DRP lookups that produced responses.
failures	Number of DRP failures (for various reasons including authentication key-chain encryption failures).

Related Commands	Command	Description
	<b>ip drp access-group</b>	Controls the sources of DRP queries to the DRP server agent.
	<b>ip drp authentication key-chain</b>	Configures authentication on the DRP server agent for DistributedDirector.

# show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

**show ip interface** [*type number*] [**brief**]

Syntax Description		
	<i>type</i>	(Optional) Interface type.
	<i>number</i>	(Optional) Interface number.
	<b>brief</b>	(Optional) Displays a summary of the usability status information for each interface.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(3)T	This command was expanded to include the status of <b>ip wccp redirect out</b> and <b>ip wccp redirect exclude add in</b> commands.
	12.2(14)S	This command was expanded to display the status of NetFlow on a subinterface.
	12.2(15)T	The command output enhancements introduced in Cisco IOS Release 12.2(14)S were integrated into Cisco IOS Release 12.2(15)T.
	12.3(6)	The command output was modified to identify the downstream VRF in the output.
	12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.

## Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface can send and receive packets. If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see information for that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

## Examples

The following example identifies a downstream VRF. The highlighted line (for documentation purposes only) identifies the downstream VRF.

```
Router# show ip interface vi 3
```

```

Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (2.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 2.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled

```

Table 21 describes the significant fields shown in the display.

**Table 21** *show ip interface Field Descriptions*

Field	Description
Virtual-Access3 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Displays the broadcast address.
Peer address is	Displays the peer address.
MTU is	Displays the MTU value set on the interface.
Helper address	Displays a helper address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.

Table 21 show ip interface Field Descriptions (continued)

Field	Description
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	Specifies the IP Security Option (IPSO) security level set for this interface.
Split horizon	Indicates that split horizon is enabled.
ICMP redirects	Specifies whether redirect messages will be sent on this interface.
ICMP unreachable	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Specifies whether Flow switching is enabled for this interface.
IP CEF switching	Specifies whether Cisco Express Forwarding (CEF) is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Specifies the VRF where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Specifies whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Specifies whether NetFlow has been enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the <b>ip flow ingress</b> command. Specifies "Flow" to specify that NetFlow is enabled on a main interface using the <b>ip route-cache flow</b> command.
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
WCCP Redirect outbound is disabled	Indicates the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Indicates the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."

The following is sample output from the **show ip interface brief** command:

```
Router# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	151.108.0.5	YES	NVRAM	up	up
Ethernet1	unassigned	YES	unset	administratively down	down
Loopback0	152.108.20.5	YES	NVRAM	up	up
Serial0	162.108.10.5	YES	NVRAM	up	up
Serial1	162.108.4.5	YES	NVRAM	up	up
Serial2	152.108.10.5	YES	manual	up	up
Serial3	unassigned	YES	unset	administratively down	down

The method field has the following possible values:

- RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request
- BOOTP—Bootstrap protocol
- TFTP—Configuration file obtained from Trivial File Transfer Protocol (TFTP) server
- manual—Manually changed by CLI command
- NVRAM—Configuration file in nonvolatile RAM (NVRAM)
- IPCP—**ip address negotiated** command
- DHCP—**ip address dhcp** command
- unassigned—No IP address
- unset—Unset
- other—Unknown



# show ip irdp

To display ICMP Router Discovery Protocol (HRDP) values, use the **show ip irdp** EXEC command.

**show ip irdp**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Modes** EXEC

---

Command History	Release	Modification
	10.0	This command was introduced.

---



---

**Examples** The following is sample output from the **show ip irdp** command:

```
Router# show ip irdp
```

```
Ethernet 0 has router discovery enabled
```

```
Advertisements will occur between every 450 and 600 seconds.
```

```
Advertisements are valid for 1800 seconds.
```

```
Default preference will be 100.
```

```
--More--
```

```
Serial 0 has router discovery disabled
```

```
--More--
```

```
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less obvious lines of output in the display are as follows:

Advertisements will occur between every 450 and 600 seconds.

This indicates the configured minimum and maximum advertising interval for the interface.

Advertisements are valid for 1800 seconds.

This indicates the configured holdtime values for the interface.

Default preference will be 100.

This indicates the configured (or in this case default) preference value for the interface.

---

Related Commands	Command	Description
	<b>ip irdp</b>	Enables IRDP processing on an interface.

---

# show ip masks

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks** EXEC command.

**show ip masks** *address*

<b>Syntax Description</b>	<i>address</i>	Network address for which a mask is required.
---------------------------	----------------	---

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Usage Guidelines** The **show ip masks** command is useful for debugging when a variable-length subnet mask (VLSM) is used. It shows the number of masks associated with the network and the number of routes for each mask.

**Examples** The following is sample output from the **show ip masks** command:

```
Router# show ip masks 131.108.0.0

Mask           Reference count
255.255.255.255 2
255.255.255.0  3
255.255.0.0     1
```

# show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics EXEC** command.

## show ip nat statistics

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	11.2	This command was introduced.

**Examples** The following is sample output from the **show ip nat statistics** command:

```
Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
  pool net-208: netmask 255.255.255.240
    start 171.69.233.208 end 171.69.233.221
    type generic, total addresses 14, allocated 2 (14%), misses 0
```

[Table 22](#) describes the significant fields shown in the display.

**Table 22** *show ip nat statistics Field Descriptions*

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the <b>ip nat outside</b> command.
Inside interfaces	List of interfaces marked as inside with the <b>ip nat inside</b> command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.

Table 22 *show ip nat statistics Field Descriptions (continued)*

Field	Description
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

## Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Changes the amount of time after which NAT translations time out.
<b>show ip nat translations</b>	Displays active NAT translations.

# show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in EXEC mode.

```
show ip nat translations [esp] [icmp] [pptp] [tcp] [udp] [verbose] [vrf vrf-name]
```

## Syntax Description

<b>esp</b>	(Optional) Displays Encapsulating Security Payload (ESP) entries.
<b>icmp</b>	(Optional) Displays Internet Control Message Protocol (ICMP) entries.
<b>pptp</b>	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) entries.
<b>tcp</b>	(Optional) Displays TCP protocol entries.
<b>udp</b>	(Optional) Displays User Datagram Protocol (UDP) entries.
<b>verbose</b>	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
<b>vrf vrf-name</b>	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

## Command Modes

EXEC

## Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The <b>vrf vrf-name</b> keyword and argument combination was added.
12.2(15)T	The <b>esp</b> keyword was added.

## Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Router# show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
--- 10.69.233.209      192.168.1.95      ---                ---
--- 10.69.233.210      192.168.1.89      ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Router# show ip nat translations
```

```
Pro Inside global      Inside local      Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.69.2.132:53    172.69.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.69.1.220:23    172.69.1.220:23
tcp 10.69.233.209:1067  192.168.1.95:1067  172.69.1.161:23    172.69.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Router# show ip nat translations verbose
```

```

Pro Inside global      Inside local      Outside local      Outside global
udp 172.69.233.209:1220 192.168.1.95:1220 172.69.2.132:53    172.69.2.132:53
      create 00:00:02, use 00:00:00, flags: extended
tcp 172.69.233.209:11012 192.168.1.89:11012 172.69.1.220:23    172.69.1.220:23
      create 00:01:13, use 00:00:50, flags: extended
tcp 172.69.233.209:1067 192.168.1.95:1067 172.69.1.161:23    172.69.1.161:23
      create 00:00:02, use 00:00:00, flags: extended

```

The following is sample output that includes the **vrf** keyword:

```

Router# show ip nat translations vrf red
Pro Inside global      Inside local      Outside local      Outside global
--- 2.2.2.1            192.168.121.113  ---              ---
--- 2.2.2.2            192.168.122.49  ---              ---
--- 2.2.2.11           192.168.11.1    ---              ---
--- 2.2.2.12           192.168.11.3    ---              ---
--- 2.2.2.13           140.48.5.20     ---              ---

Pro Inside global      Inside local      Outside local      Outside global
--- 2.2.2.3            192.168.121.113  ---              ---
--- 2.2.2.4            192.168.22.49   ---              ---

```

The following is sample output that includes the **esp** keyword:

```

Router# show ip nat translations esp
Pro Inside global      Inside local      Outside local      Outside global
esp 192.168.22.40:0    192.168.122.20:0 192.168.22.20:0
192.168.22.20:28726CD9
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0

```

The following is sample output that includes the **esp** and **verbose** keywords:

```

Router# show ip nat translation esp verbose
Pro Inside global      Inside local      Outside local      Outside global
esp 192.168.22.40:0    192.168.122.20:0 192.168.22.20:0
192.168.22.20:28726CD9
      create 00:00:00, use 00:00:00,
      flags:
      extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0
      create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
      flags:
      extended, use_count:0, entry-id:191, lc_entries:0

```

Table 23 describes the significant fields shown in the display.

**Table 23** show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.

Table 23 *show ip nat translations Field Descriptions (continued)*

Field	Description
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: <ul style="list-style-type: none"> <li>• extended—Extended translation</li> <li>• static—Static translation</li> <li>• destination—Rotary translation</li> <li>• outside—Outside translation</li> <li>• timing out—Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.</li> </ul>

## Related Commands

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.

# show ip nhrp

To display the Next Hop Resolution Protocol (NHRP) cache, use the **show ip nhrp** EXEC command.

```
show ip nhrp [ip-address ip-address [brief]] [dynamic | static | incomplete | nhs type number]
[detail | purge]
```

Syntax Description		
<b>ip-address</b>	(Optional) Displays the cache for a specified destination prefix. The <i>ip-address</i> argument specifies the IP address.	
<b>brief</b>	(Optional) Display a single line of output per cache entry.	
<b>dynamic</b>	(Optional) Displays only the dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) cache entries. See <a href="#">Table 23</a> for types, number ranges, and descriptions.	
<b>static</b>	(Optional) Displays only the static IP-to-NBMA address entries in the cache (configured using the <b>ip nhrp map</b> command). See <a href="#">Table 23</a> for types, number ranges, and descriptions.	
<b>incomplete</b>	(Optional) Displays information about an incomplete cache. See <a href="#">Table 23</a> for types, number ranges, and descriptions.	
<b>nhs</b>	(Optional) Displays information about the next-hop server (NHS). See <a href="#">Table 23</a> for types, number ranges, and descriptions.	
<i>type number</i>	(Optional) Displays the interface type and number in the NHRP cache. See <a href="#">Table 23</a> for types, number ranges, and descriptions.	
<b>detail</b>	(Optional) Displays detailed information about NHRP cache.	
<b>purge</b>	(Optional) Displays NHRP cache purge information.	

Command Modes EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.3(11)T	The <b>ip-address</b> and <b>brief</b> keywords were added.

**Usage Guidelines** [Table 23](#) lists the valid types, number ranges, and descriptions for the *type* and *number* optional arguments.

**Table 23 Valid Types, Number Ranges, and Interface Descriptions**

Valid Types	Number Ranges	Interface Descriptions
<b>atm</b>	0 to 6	ATM
<b>async</b>	1	Async
<b>bvi</b>	1 to 255	Bridge-Group Virtual Interface
<b>cdma-ix</b>	1	CDMA Ix



**Table 23 Valid Types, Number Ranges, and Interface Descriptions (continued)**

Valid Types	Number Ranges	Interface Descriptions
<b>ctunnel</b>	0 to 2147483647	C-Tunnel
<b>dialer</b>	0 to 20049	Dialer
<b>fastethernet</b>	0 to 6	FastEthernet IEEE 802.3
<b>lex</b>	0 to 2147483647	Lex
<b>loopback</b>	0 to 2147483647	Loopback
<b>mfr</b>	0 to 2147483647	Multilink Frame Relay bundle
<b>multilink</b>	0 to 2147483647	Multilink-group
<b>null</b>	0	Null
<b>port-channel</b>	1 to 64	Port channel
<b>tunnel</b>	0 to 2147483647	Tunnel
<b>vif</b>	1	PGM multicast host
<b>virtual-ppp</b>	0 to 2147483647	Virtual PPP
<b>virtual-template</b>	1 to 1000	Virtual template
<b>virtual-tokenring</b>	0 to 2147483647	Virtual Token Ring
<b>xtagatm</b>	0 to 2147483647	Extended tag ATM

**Examples**

The following is sample output from the **show ip nhrp** command:

```
Router# show ip nhrp

10.0.0.2 255.255.255.255, ATM0/0 created 0:00:43 expire 1:59:16
  Type: dynamic Flags: authoritative
  NBMA address: 11.1111.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
  Type: static Flags: authoritative
  NBMA address: 11.1.1.2
```

[Table 24](#) describes the significant fields shown in the display.

**Table 24 show ip nhrp Field Descriptions**

Field	Description
10.0.0.2 255.255.255.255	IP address and its network mask in the IP-to-NBMA address cache. The mask is currently always 255.255.255.255 because we do not support aggregation of NBMA information through NHRP.
ATM0/0 created 0:00:43	Interface type and number (in this case, ATM slot and port numbers) and how long ago it was created (hours:minutes:seconds).
expire 1:59:16	Time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the <b>ip nhrp holdtime</b> command.

Table 24 *show ip nhrp Field Descriptions (continued)*

Field	Description
Type	<ul style="list-style-type: none"> <li>dynamic—NBMA address was obtained from NHRP Request packet.</li> <li>static—NBMA address was statically configured.</li> </ul>
Flags	<ul style="list-style-type: none"> <li>authoritative—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IP address mapping for a particular destination.</li> <li>implicit—Indicates that the information was learned not from an NHRP request generated from the local router, but from an NHRP packet being forwarded or from an NHRP request being received by the local router.</li> <li>negative—For negative caching; indicates that the requested NBMA mapping could not be obtained.</li> </ul>
NBMA address	Nonbroadcast multiaccess address. The address format is appropriate for the type of network being used (for example, ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel).

## Related Commands

Command	Description
<b>ip nhrp map</b>	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
<b>show ip nhrp traffic</b>	Displays NHRP traffic statistics.

# show ip nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ip nhrp traffic** EXEC command.

## show ip nhrp traffic

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	10.3	This command was introduced.

**Examples** The following is sample output from the **show ip nhrp traffic** command:

```
Router# show ip nhrp traffic

Tunnel0
  request packets sent: 2
  request packets received: 4
  reply packets sent: 4
  reply packets received: 2
  register packets sent: 0
  register packets received: 0
  error packets sent: 0
  error packets received: 0
```

[Table 25](#) describes the significant fields shown in the display.

**Table 25** *show ip nhrp traffic Field Descriptions*

Field	Description
Tunnel 0	Interface type and number.
request packets sent	Number of NHRP request packets originated from this station.
request packets received	Number of NHRP request packets received by this station.
reply packets sent	Number of NHRP reply packets originated from this station.
reply packets received	Number of NHRP reply packets received by this station.
register packets sent	Number of NHRP register packets originated from this station. Currently, our routers and access servers do not send register packets, so this value is 0.
register packets received	Number of NHRP register packets received by this station. Currently, our routers or access servers do not send register packets, so this value is 0.

**Table 25** *show ip nhrp traffic Field Descriptions (continued)*

Field	Description
error packets sent	Number of NHRP error packets originated by this station.
error packets received	Number of NHRP error packets received by this station.

# show ip redirects

To display the address of a default gateway (router) and the address of hosts for which an Internet Control Message Protocol (ICMP) redirect message has been received, use the **show ip redirects** command in user EXEC or privileged EXEC mode.

## show ip redirects

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** This command displays the default router (gateway) as configured by the **ip default-gateway** command. The **ip mtu** command enables the router to send ICMP redirect messages.

**Examples** The following is sample output from the **show ip redirects** command:

```
Router# show ip redirects

Default gateway is 160.89.80.29

Host          Gateway          Last Use      Total Uses   Interface
131.108.1.111 160.89.80.240    0:00         9    Ethernet0
128.95.1.4    160.89.80.240    0:00         4    Ethernet0
Router#
```

Related Commands	Command	Description
	<b>ip default-gateway</b>	Defines a default gateway (router) when IP routing is disabled.
	<b>ip mtu</b>	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.

# show ip route dhcp

To display the routes added to the routing table by the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server and relay agent, use the **show ip route dhcp** command in privileged EXEC configuration mode.

```
show ip route [vrf vrf-name] dhcp [ip-address]
```

Syntax Description	Parameter	Description
	<b>vrf</b>	(Optional) Specifies VPN routing and forwarding instance.
	<i>vrf-name</i>	(Optional) Name of the VRF.
	<i>ip-address</i>	(Optional) Address about which routing information should be displayed.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2	This command was introduced.

**Usage Guidelines** To display information about global routes, use the **show ip route dhcp** command. To display routes in the VRF routing table, use the **show ip route vrf vrf-name dhcp** command.

**Examples** The following is sample output from the **show ip route dhcp** command when entered without an address. This command lists all routes added by the Cisco IOS DHCP server and relay agent.

```
Router# show ip route dhcp
 55.5.5.56/32 is directly connected, ATM0.2
 55.5.5.217/32 is directly connected, ATM0.2
```

The following is sample output from the **show ip route dhcp** command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route dhcp 55.5.5.217
 55.5.5.217 is directly connected, ATM0.2
   DHCP Server: 49.9.9.10   Lease expires at Nov 08 2001 01:19 PM
```

The following is sample output from the **show ip route vrf vrf-name dhcp** command when entered without an address:

```
Router# show ip route vrf red dhcp
 55.5.5.218/32 is directly connected, ATM0.2
```

## ■ show ip route dhcp

The following is sample output from the **show ip route vrf vrf-name dhcp** command when an address is specified. The output shows the details of the address with the server address (who assigned it) and the lease expiration time.

```
Router# show ip route vrf red dhcp 55.5.5.218
55.5.5.218/32 is directly connected, ATM0.2
  DHCP Server: 49.9.9.10   Lease expires at Nov 08 2001 03:15PM
```

---

**Related Commands**

Command	Description
<b>clear ip route dhcp</b>	Removes routes from the routing table added by the DHCP server and relay agent for the DHCP clients on unnumbered interfaces.

# show ip slb conns

To display the active IOS SLB connections, use the **show ip slb conns** privileged EXEC command.

**show ip slb conns** [*vserver* *virtserver-name*] [*client* *ip-address*] [**detail**]

Syntax Description		
<b>vserver</b>	(Optional)	Displays only those connections associated with a particular virtual server.
<i>virtserver-name</i>	(Optional)	Name of the virtual server to be monitored.
<b>client</b>	(Optional)	Displays only those connections associated with a particular client IP address.
<i>ip-address</i>	(Optional)	IP address of the client to be monitored.
<b>detail</b>	(Optional)	Displays detailed connection information.

**Defaults** If no options are specified, the command displays output for all active IOS SLB connections.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows IOS SLB active connection data:

```
router# show ip slb conns
```

```

vserver      prot  client                               real                               state
-----
TEST         TCP   7.150.72.183:328                    80.80.90.25:80                    CLOSING
TEST         TCP   7.250.167.226:423                    80.80.90.26:80                    CLOSING
TEST         TCP   7.234.60.239:317                     80.80.90.26:80                    CLOSING
TEST         TCP   7.110.233.96:747                     80.80.90.26:80                    CLOSING
TEST         TCP   7.162.0.201:770                      80.80.90.30:80                    CLOSING
TEST         TCP   7.22.225.219:995                     80.80.90.26:80                    CLOSING
TEST         TCP   7.2.170.148:169                      80.80.90.30:80                    CLOSING

```

[Table 26](#) describes the significant fields shown in the display.



**Table 26** *show ip slb conns Field Descriptions*

Field	Description
vserver	Name of the virtual server whose connections are being monitored and displayed. Information about each connection is displayed on a separate line.
prot	Protocol being used by the connection.
client	Client IP address being used by the connection.
real	Real IP address of the connection.
state	<p>Current state of the connection:</p> <ul style="list-style-type: none"> <li>• CLOSING—IOS SLB TCP connection deactivated (awaiting a delay timeout before cleaning up the connection).</li> <li>• ESTAB—IOS SLB TCP connection processed a SYN-SYN/ACK exchange between the client and server.</li> <li>• FINCLIENT—IOS SLB TCP connection processed a FIN from the client.</li> <li>• FINSERVER—IOS SLB TCP connection processed a FIN from the server.</li> <li>• INIT—Initial state of the IOS SLB TCP connection.</li> <li>• SYNBOTH—IOS SLB TCP connection processed one or more TCP SYNs from both the client and the server.</li> <li>• SYNCLIENT—IOS SLB TCP connection processed one or more client TCP SYNs.</li> <li>• SYNSERVER—IOS SLB TCP connection processed one or more server 1 TCP SYNs.</li> <li>• ZOMBIE—Destruction of the IOS SLB TCP connection failed, possibly because of bound flows. Destruction will proceed when the flows are unbound.</li> </ul>

# show ip slb dfp

To display DFP manager and agent information such as passwords, timeouts, retry counts, and weights, use the **show ip slb dfp** privileged EXEC command.

**show ip slb dfp** [*agent ip-address port-number* | **detail** | **weights**]

Syntax Description	
<b>agent</b>	(Optional) Displays information about an agent.
<i>ip-address</i>	(Optional) Agent IP address.
<i>port-number</i>	(Optional) Agent port number.
<b>detail</b>	(Optional) Displays all data available.
<b>weights</b>	(Optional) Displays information about weights assigned to real servers for load balancing.

**Defaults** If no options are specified, the command displays summary information.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows IOS SLB DFP data:

```
router# show ip slb dfp detail

DFP Manager:
  Current passwd:NONE Pending passwd:NONE
  Passwd timeout:0 sec
  Uned errors:0
DFP Agent 161.44.2.34:61936 Connection state:Connected
  Timeout = 0      Retry Count = 0      Interval = 180      (Default)
  Security errors = 0
  Last message received:10:20:26 UTC 11/02/99
  Last reported Real weights for Protocol TCP, Port www
    Host 17.17.17.17 1      Weight 1
    Host 68.68.68.68  Bind ID 4      Weight 4
    Host 85.85.85.85  Bind ID 5      Weight 5
  Last reported Real weights for Protocol TCP, Port 22
    Host 17.17.17.17  Bind ID 111     Weight 111

router# show ip slb dfp weights

Real IP Address 17.17.17.17 Protocol TCP Port 22 Bind_ID 111 Weight 111
  Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
Real IP Address 17.17.17.17 Protocol TCP Port www Bind_ID 1 Weight 1
  Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
```

■ `show ip slb dfp`

```
Real IP Address 68.68.68.68 Protocol TCP Port www Bind_ID 4 Weight 4
  Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
Real IP Address 85.85.85.85 Protocol TCP Port www Bind_ID 5 Weight 5
  Set by Agent 161.44.2.3458490 at 132241 UTC 12/03/99
```

```
router# show ip slb dfp
```

```
DFP Manager:
  Current passwd:NONE Pending passwd:NONE
  Passwd timeout:0 sec
```

```
Agent IP          Port      Timeout  Retry Count  Interval
-----
161.44.2.34      61936    0        0            180 (Default)
```

[Table 27](#) describes the significant fields shown in the display.

**Table 27** *show ip slb dfp* Field Descriptions

Field	Description
Agent IP	IP address of the agent about which information is being displayed.
Port	Port number of the agent.
Timeout	Time period (in seconds) during which the DFP manager must receive an update from the DFP agent. A value of 0 means there is no timeout.
Retry Count	Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. A value of 0 means there are infinite retries.
Interval	Interval (in seconds) between retries.

# show ip slb reals

To display information about the real servers, use the **show ip slb reals** privileged EXEC command.

**show ip slb reals** [**vserver** *virtserver-name*] [**detail**]

Syntax Description		
<b>vserver</b>	(Optional)	Displays information about only those real servers associated with a particular virtual server.
<i>virtserver-name</i>	(Optional)	Name of the virtual server.
<b>detail</b>	(Optional)	Displays detailed information.

**Defaults** If no options are specified, the command displays information about all real servers.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows IOS SLB real server data:

```
router# show ip slb reals
```

```

real          server farm    weight  state          conns
-----
80.80.2.112   FRAG          8       OUTOFSERVICE  0
80.80.5.232   FRAG          8       OPERATIONAL   0
80.80.15.124  FRAG          8       OUTOFSERVICE  0
80.254.2.2    FRAG          8       OUTOFSERVICE  0
80.80.15.124  LINUX        8       OPERATIONAL   0
80.80.15.125  LINUX        8       OPERATIONAL   0
80.80.15.126  LINUX        8       OPERATIONAL   0
80.80.90.25   SRE          8       OPERATIONAL   220
80.80.90.26   SRE          8       OPERATIONAL   216
80.80.90.27   SRE          8       OPERATIONAL   216
80.80.90.28   SRE          8       TESTING       1
80.80.90.29   SRE          8       OPERATIONAL   221
80.80.90.30   SRE          8       OPERATIONAL   224
80.80.30.3    TEST        100      READY_TO_TEST 0
80.80.30.4    TEST        100      READY_TO_TEST 0
80.80.30.5    TEST        100      READY_TO_TEST 0
80.80.30.6    TEST        100      READY_TO_TEST 0

```

[Table 28](#) describes significant fields shown in the display.

**Table 28** *show ip slb reals Field Descriptions*

Field	Description
real	IP address of the real server about which information is being displayed. Used to identify each real server. Information about each real server is displayed on a separate line.
server farm	Name of the server farm to which the real server is associated.
weight	Weight assigned to the real server. The weight identifies the capacity of the real server, relative to other real servers in the server farm.
state	Current state of the real server: <ul style="list-style-type: none"> <li>• DFP_THROTTLED—DFP agent sent a weight of 0 for this real server (send no further connections to this real server).</li> <li>• FAILED—Removed from use by the predictor algorithms; retry timer started.</li> <li>• MAXCONNS—Maximum number of simultaneous active connections reached.</li> <li>• OPERATIONAL—Functioning properly.</li> <li>• OUTOFSERVICE—Removed from the load-balancing predictor lists.</li> <li>• READY_TO_TEST—Queued for testing.</li> <li>• TESTING—Queued for assignment.</li> </ul>

# show ip slb serverfarms

To display information about the server farms, use the **show ip slb serverfarms** privileged EXEC command.

**show ip slb serverfarms** [*name serverfarm-name*] [*detail*]

Syntax Description	name	(Optional) Displays information about only a particular server farm.
	<i>serverfarm-name</i>	(Optional) Name of the server farm.
	<b>detail</b>	(Optional) Displays detailed server farm information.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows IOS SLB server farm data:

```
router# show ip slb serverfarms

server farm      predictor      reals    bind id
-----
FRAG             ROUNDROBIN    4        0
LINUX            ROUNDROBIN    3        0
SRE              ROUNDROBIN    6        0
TEST             ROUNDROBIN    4        0
```

[Table 29](#) describes the significant fields shown in the display.

**Table 29** *show ip slb serverfarms* Field Descriptions

Field	Description
server farm	Name of the server farm about which information is being displayed. Information about each server farm is displayed on a separate line.
predictor	Type of load-balancing algorithm (ROUNDROBIN or LEASTCONNS) used by the server farm.
reals	Number of real servers configured in the server farm.
bind id	Bind ID configured on the server farm.

# show ip slb stats

To display IOS SLB statistics, use the **show ip slb stats** privileged EXEC command.

## show ip slb stats

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows IOS SLB statistics:

```
router# show ip slb stats

Pkts via normal switching: 530616
Pkts via special switching:1812710
Connections Created:      783774
Connections Established:  633418
Connections Destroyed:   782752
Connections Reassigned:   0
Zombie Count:            0
```

[Table 30](#) describes the significant fields shown in the display.

**Table 30** *show ip slb stats Field Descriptions*

Field	Description
Pkts via normal switching	Number of packets handled by the IOS SLB feature via normal switching since the last time counters were cleared.
Pkts via special switching	Number of packets handled by the IOS SLB feature via special switching since the last time counters were cleared.
Connections Created	Number of connections created since the last time counters were cleared.
Connections Established	Number of connections created that have become established since the last time counters were cleared.
Connections Destroyed	Number of connections destroyed since the last time counters were cleared.

**Table 30** *show ip slb stats Field Descriptions (continued)*

Connections Reassigned	Number of connections reassigned to a different real server since the last time counters were cleared.
Zombie Count	Number of connections currently pending destruction, awaiting a timeout or some other condition to be met.



# show ip slb sticky

To display the entries in the IOS SLB sticky database, use the **show ip slb sticky** privileged EXEC command.

```
show ip slb sticky [client ip-address]
```

Syntax Description	client	(Optional) Displays only those sticky database entries associated with a particular client IP address.
	<i>ip-address</i>	(Optional) IP address of the client.

**Defaults** If no options are specified, the command displays information about all virtual servers.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows the entries in the IOS SLB sticky database:

```
router# show ip slb sticky

client          group  real          conns  ftp-cntrl
-----
10.10.2.12      4097  10.10.3.2    1      0
```

[Table 31](#) describes the significant fields shown in the display.

**Table 31** *show ip slb sticky* Field Descriptions

Field	Description
client	Client IP address that is bound to this sticky assignment.
group	Group ID for this sticky assignment.
real	Real server used by all clients connecting with the client IP address detailed on this line.
conns	Number of connections currently sharing this sticky assignment.
ftp-cntrl	Number of FTP control connections currently using this sticky assignment.

# show ip slb vservers

To display information about the virtual servers, use the **show ip slb vservers** privileged EXEC command.

**show ip slb vservers** [**name** *virtserver-name*] [**detail**]

Syntax Description	name	(Optional) Displays information about only this virtual server.
	<i>virtserver-name</i>	(Optional) Name of the virtual server.
	<b>detail</b>	(Optional) Displays detailed virtual server information.

**Defaults** If no options are specified, the command displays information about all virtual servers.

**Command Modes** Privileged EXEC

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

**Examples** The following example shows virtual server data:

```
router# show ip slb vservers

slb vserver      prot  virtual                               state      conns
-----
TEST             TCP   80.80.254.3:80                       OPERATIONAL 1013
TEST21          TCP   80.80.254.3:21                       OUTOFSERVICE 0
TEST23          TCP   80.80.254.3:23                       OUTOFSERVICE 0
```

[Table 32](#) describes the significant fields shown in the display.

**Table 32** *show ip slb vservers* Field Descriptions

Field	Description
slb vserver	Name of the virtual server about which information is being displayed. Information about each virtual server is displayed on a separate line.
prot	Protocol being used by the virtual server detailed on a given line.
virtual	Virtual IP address of the virtual server detailed on a given line.
state	Current state of the virtual server detailed on a given line.
conns	Number of connections associated with the virtual server detailed on a given line.

# show ip snat

To display active Stateful Network Address Translation (SNAT) translations, use the **show ip snat** command in EXEC mode.

**show ip snat** [**distributed** [**verbose**] | **peer** *ip-address*]

Syntax Description		
	<b>distributed</b>	(Optional) Displays information about the distributed NAT, including its peers and status.
	<b>verbose</b>	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
	<b>peer</b> <i>ip-address</i>	(Optional) Displays TCP connection information between peer routers.

**Command Modes** EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

## Examples

The following is sample output from the **show ip snat distributed** command for stateful NAT connected peers:

```
Router# show ip snat distributed

Stateful NAT Connected Peers

SNAT: Mode PRIMARY
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
```

The following is sample output from the **show ip snat distributed verbose** command for stateful NAT connected peers:

```
Router# show ip snat distributed verbose
```

```
SNAT: Mode PRIMARY
```

```
Stateful NAT Connected Peers
```

```
:State READY
```

```
:Local Address 192.168.123.2
```

```
:Local NAT id 100
```

```
:Peer Address 192.168.123.3
```

```
:Peer NAT id 200
```

```
:Mapping List 10
```

```
:InMsgs 7, OutMsgs 7, tcb 0x63EBA408, listener 0x0
```

# show ip sockets

To display IP socket information, use the **show ip sockets** command in user EXEC or privileged EXEC mode.

## show ip sockets

**Syntax Description** This command has no keywords or arguments.

**Defaults** No default behavior or values.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	10.0 T	This command was introduced.

**Usage Guidelines** Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

**Examples** The following is sample output from the **show ip sockets** command:

```
Router# show ip sockets
```

```
Proto  Remote      Port      Local          Port  In Out Stat TTY OutputIF
17     0.0.0.0     0         171.68.186.193  67   0  0   1  0
17     171.68.191.135 514      171.68.191.129 1811  0  0   0  0
17     172.16.135.20 514      171.68.191.1   4125  0  0   0  0
17     171.68.207.163 49       171.68.186.193  49   0  0   9  0
17     0.0.0.0     123      171.68.186.193 123   0  0   1  0
88     0.0.0.0     0         171.68.186.193 202   0  0   0  0
17     172.16.96.59 32856    171.68.191.1   161   0  0   1  0
17     --listen--           --any--          496   0  0   1  0
```

[Table 33](#) describes the significant fields shown in the display.

**Table 33** *show ip sockets Field Descriptions*

Field	Description
Proto	Protocol type, for example, User Datagram Protocol (UDP) or TCP.
Remote	Remote address connected to this networking device. If the remote address is considered illegal, "--listen--" is displayed.
Port	Remote port. If the remote address is considered illegal, "--listen--" is displayed.

**Table 33** *show ip sockets Field Descriptions (continued)*

Field	Description
Local	Local address. If the local address is considered illegal or is the address 0.0.0.0, "--any--" displays.
Port	Local port.
In	Input queue size.
Out	Output queue size.
Stat	Various statistics for a socket.
TTY	The tty number for the creator of this socket.
OutputIF	Output IF string, if one exists.

# show ip traffic

To display statistics about IP traffic, use the **show ip traffic** command in user EXEC or privileged EXEC mode.

## show ip traffic

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

**Examples** The following is sample output from the **show ip traffic** command:

```
Router# show ip traffic

IP statistics:
  Rcvd: 98 total, 98 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
        0 fragmented, 0 couldn't fragment
  Bcast: 38 received, 52 sent
  Sent: 44 generated, 0 forwarded
        0 encapsulation failed, 0 no route
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
        0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 3 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 56 total, 0 checksum errors, 55 no port
  Sent: 18 total, 0 forwarded broadcasts
TCP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
EGP statistics:
  Rcvd: 0 total, 0 format errors, 0 checksum errors, 0 no listener
  Sent: 0 total
IGRP statistics:
  Rcvd: 73 total, 0 checksum errors
  Sent: 26 total
HELLO statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 20 requests, 17 replies, 0 reverse, 0 other
```

```

    Sent: 0 requests, 9 replies (0 proxy), 0 reverse
Probe statistics:
  Rcvd: 6 address requests, 0 address replies
0 proxy name requests, 0 other
  Sent: 0 address requests, 4 address replies (0 proxy)
        0 proxy name replies

```

Table 34 describes the significant fields shown in the display.

**Table 34** *show ip traffic Field Descriptions*

Field	Description
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
bad hop count	Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
no route	Counted when the Cisco IOS software discards a datagram it did not know how to route.
proxy name replies	Counted when the Cisco IOS software sends an ARP request or Probe Reply on behalf of another host. The display shows the number of probe proxy requests that have been received and the number of responses that have been sent.



# show ip wccp

To display global statistics related to Web Cache Communication Protocol (WCCP), use the **show ip wccp** command in privileged EXEC mode.

```
show ip wccp [service-number [detail | view] | web-cache [detail | view]]
```

Syntax Description	
<i>service-number</i>	(Optional) Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 99. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of <b>99</b> .
<b>web-cache</b>	(Optional) Statistics for the web-cache service.
<b>detail</b>	(Optional) Information about the router and all web caches.
<b>view</b>	(Optional) Other members of a particular service group have or have not been detected.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	11.1 CA	This command was introduced for Cisco 7200 and 7500 platforms.
	11.2 P	Support for this command was added to a variety of Cisco platforms.
	12.0(3)T	The <b>detail</b> and <b>view</b> keywords were added.
	12.3(7)T	The output was enhanced to display the bypass counters (process, fast, and Cisco Express Forwarding) when WCCP is enabled.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines	
	Use the <b>clear ip wccp</b> command to reset the counter for the “Packets Redirected” information.

Examples	
	This section contains examples and field descriptions for four forms of this command:

- **show ip wccp web-cache**
- **show ip wccp** *service-number* **view**
- **show ip wccp web-cache detail**
- **show ip wccp web-cache detail** (bypass counters displayed)

```
show ip wccp web-cache
```

The following is sample output from the **show ip wccp web-cache** command:

```
Router# show ip wccp web-cache
```

```
Global WCCP Information:
Service Name: web-cache:
Number of Cache Engines:1
Number of Routers:1
```

```

Total Packets Redirected:213
Redirect access-list:no_linux
Total Packets Denied Redirect:88
Total Packets Unassigned:-none-
Group access-list:0
Total Messages Denied to Group:0
Total Authentication failures:0

```

Table 35 describes the significant fields shown in the display.

**Table 35** *show ip wccp web-cache Field Descriptions*

Field	Description
Service Name	Indicates which service is detailed.
Number of Cache Engines	Number of Cisco cache engines using the router as their home router.
Number of Routers	The number of routers in the service group.
Total Packets Redirected	Total number of packets redirected by the router.
Redirect access-list	The name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any cache engine. Packets may not be assigned during initial discovery of cache engines or when a cache is dropped from a cluster.
Group access-list	Indicates which cache engine is allowed to connect to the router.
Total Messages Denied to Group	Indicates the number of messages disallowed by the router because they did not meet all the requirements of the service group.
Total Authentication failures	The number of instances where a password did not match.

#### **show ip wccp service-number view**

The following is sample output from the **show ip wccp 1 view** command:

```

Router# show ip wccp 1 view

WCCP Router Informed of:
 10.168.88.10
 10.168.88.20

WCCP Cache Engines Visible
 10.168.88.11
 10.168.88.12

WCCP Cache Engines Not Visible:
 -none-

```

If any web cache is displayed under the WCCP Cache Engines Not Visible field, the router needs to be reconfigured to map the web cache that is not visible to it.

Table 36 describes the significant fields shown in the display.

**Table 36** *show ip wccp service-number view Field Descriptions*

Field	Description
WCCP Router Informed of	A list of routers detected by the current router.
WCCP Cache Engines Visible	A list of cache engines that are visible to the router and other cache engines in the service group.
WCCP Cache Engines Not Visible	A list of cache engines in the service group that are not visible to the router and other cache engines in the service group.

**show ip wccp web-cache detail**

The following example displays web-cache engine information and WCCP router statistics for a particular service group:

```
Router# show ip wccp web-cache detail

WCCP Router information:
  IP Address:10.168.88.10
  Protocol Version:2.0

WCCP Cache-Engine Information
  IP Address:10.168.88.11
  Protocol Version:2.0
  State:Usable
  Initial Hash Info:AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAA
Assigned Hash Info:FFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment:256 (100.00%)
Packets Redirected:21345
Connect Time:00:13:46
```

[Table 37](#) describes the significant fields shown in the display.

**Table 37** *show ip wccp detail Field Descriptions*

Field	Description
WCCP Router information	The header for the area that contains fields for the IP address and version of WCCP associated with the router connected to the cache engine in the service group.
IP Address	The IP address of the router connected to the cache engine in the service group.
Protocol Version	The version of WCCP being used by the router in the service group.
WCCP Cache Engine Information	Contains fields for information on cache engines.
IP Address	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Initial Hash Info	The initial state of the hash bucket assignment.

**Table 37** *show ip wccp detail Field Descriptions (continued)*

Field	Description
Assigned Hash Info	The current state of the hash bucket assignment.
Hash Allotment	The percent of buckets assigned to the current cache engine. Both a value and a percent figure are displayed.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time it took for the cache engine to connect to the router.

**show ip wccp web-cache detail (Bypass Counters)**

The following example displays web-cache engine information and WCCP router statistics that include the bypass counters:

```
Router# show ip wccp web-cache detail
```

```
WCCP Router information:
  IP Address:10.168.88.10
  Protocol Version:2.0

WCCP Cache-Engine Information
  IP Address:10.168.88.11
  Protocol Version:2.0
  State:Usable
  Initial Hash Info:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  Assigned Hash Info:FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  Hash Allotment:256 (100.00%)
  Packets Redirected:21345
  Connect Time:00:13:46
Bypassed Packets
  Process:          0
  Fast:             0
  CEF:              250
```

[Table 37](#) describes the significant fields shown in the display.

**Table 38** *show ip wccp web-cache detail Field Descriptions*

Field	Description
WCCP Router information	The header for the area that contains fields for the IP address and the version of WCCP associated with the router connected to the cache engine in the service group.
IP Address	The IP address of the router connected to the cache engine in the service group.
Protocol Version	The version of WCCP that is being used by the router in the service group.
WCCP Cache-Engine Information	Contains fields for information on cache engines.
IP Address	The IP address of the cache engine in the service group.
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.

**Table 38** *show ip wccp web-cache detail Field Descriptions (continued)*

Field	Description
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Initial Hash Info	The initial state of the hash bucket assignment.
Assigned Hash Info	The current state of the hash bucket assignment.
Hash Allotment	The percent of buckets assigned to the current cache engine. Both a value and a percent figure are displayed.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time that it took for the cache engine to connect to the router.
Bypassed Packets	The number of packets that have been bypassed. Process, fast, and Cisco Express Forwarding (CEF) are switching paths within Cisco IOS software.

**Related Commands**

Command	Description
<b>clear ip wccp</b>	Clears the counter for packets redirected using WCCP.
<b>ip wccp</b>	Enables WCCP on a router and specifies the type of services to be used.
<b>show ip interface</b>	Lists a summary of the IP information and status of an interface.

# show ip wccp web-caches

The **show ip wccp web-caches** command has been replaced by the **show ip wccp web-cache detail** command. See the description of the **show ip wccp** command in this book for more information.

## Command History

Release	Modification
11.2P, 11.1CA, 12.0	This command was introduced.
12.1	This command was replaced by the <b>show ip wccp</b> command.

# show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

```
show standby [type number [group-number]] [active | init | listen | standby] [brief]
```

Syntax Description	
<i>type number</i>	(Optional) Interface type and number for which output is displayed.
<i>group-number</i>	(Optional) Group number on the interface for which output is displayed.
<b>active</b>	(Optional) Displays HSRP groups in the active state.
<b>init</b>	(Optional) Displays HSRP groups in the initial state.
<b>listen</b>	(Optional) Displays HSRP groups in the listen or learn state.
<b>standby</b>	(Optional) Displays HSRP groups in the standby or speak state.
<b>brief</b>	(Optional) Summarizes each standby group in a single line of output .

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(3)T	The following keywords were added: <ul style="list-style-type: none"> <li>• <b>active</b></li> <li>• <b>init</b></li> <li>• <b>listen</b></li> <li>• <b>standby</b></li> </ul>
	12.2(8)T	The output for this command was made clearer and easier to understand.
	12.3(2)T	The output was enhanced to display information about Message Digest 5 (MD5) authentication.
	12.3(4)T	The output was enhanced to display information about HSRP version 2.

## Examples

The following is sample output from the **show standby** command when HSRP version 1 is configured:

```
Router# show standby

Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
  Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
  Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
  Next hello sent in 1.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
```

```

Active router is local
Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
Priority 95 (configured 120)
  Tracking 2 objects, 0 up
    Down Interface Ethernet0/2, pri 15
    Down Interface Ethernet0/3
IP redundancy name is "HSRP1", advertisement interval is 34 sec

```

The following is sample output from the **show standby** command with an interface and the **brief** and **init** keywords specified:

```
Router# show standby ethernet0/1 1 init brief
```

Interface	Grp	Prio	P	State	Active addr	Standby addr	Group addr
Et0	1	120		Init	10.0.0.1	unknown	10.0.0.12

The following is sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Router# show standby
```

```

Ethernet0/1 - Group 1
  State is Active
    5 state changes, last state change 00:17:27
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.276 secs
  Authentication MD5, key-string "f33r45", timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  IP redundancy name is "hsrp-Et0/1-1" (default)

```

The following is sample output from the **show standby** command when HSRP version 2 is configured:

```
Router# show standby
```

```

Ethernet0/1 - Group 1 (version 2)
  State is Speak
  Virtual IP address is 10.21.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 20 (configured 20)
  IP redundancy name is "hsrp-Et0/1-1" (default)

Ethernet0/2 - Group 1
  State is Speak
  Virtual IP address is 10.22.0.10
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.804 secs
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 90 (default 100)

```



```
Track interface Serial2/0 state Down decrement 10
IP redundancy name is "hsrp-Et0/2-1" (default)
```

Table 39 describes the significant fields shown in the displays.

**Table 39** show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface. If HSRP version 2 is configured, the version number is shown in parentheses.
State is	State of the local router; can be one of the following: <ul style="list-style-type: none"> <li>Active—Indicates the current Hot Standby router.</li> <li>Standby—Indicates the router next in line to be the Hot Standby router.</li> <li>Speak—Router is sending packets to claim the active or standby role.</li> <li>Listen—Router is not in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak.</li> <li>Learn—Router is not in the active nor standby state, nor does it have enough information to attempt to claim the active or standby roles.</li> <li>Init or Disabled—Router is not yet ready or able to participate in HSRP, possibly because the associated interface is not up. HSRP groups configured on other routers on the network that are learned via snooping are displayed as being in the Init state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state. For these cases, the Active addr and Standby addr fields will show “unknown.” The state is listed as disabled in the fields when the <b>standby ip</b> command has not been specified.</li> </ul>
Virtual IP address is, Secondary virtual IP address	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the router has failed to defend its Address Resolution Protocol (ARP) cache entry.
Active virtual MAC address is	Virtual MAC address being used by the current active router.
Local virtual MAC address is	Virtual MAC address that would be used if this router became the active router. The origin of this address (displayed in parentheses) can be “default,” “bia,” (burned-in address) or “configd” (configured).
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the <b>standby timers</b> command. The hold time is the time (in seconds) before other routers declare the active or standby router to be down, based on the <b>standby timers</b> command. All routers in an HSRP group use the hello-time and hold-time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello-time and hold-time values.
Next hello sent in	Time at which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Authentication	Authentication type configured based on the <b>standby authentication</b> command.
key-string	Key string used for authentication. Key chains are displayed if configured.

**Table 39** *show standby Field Descriptions (continued)*

Field	Description
timeout	Duration (in seconds) for which HSRP will accept message digests based on both the old and new keys.
Preemption enabled, sync delay	Indicates whether preemption is enabled. If enabled, the minimum delay is the time a higher-priority nonactive router will wait before preempting the lower-priority active router. The sync delay is the maximum time (in seconds) a group will wait to synchronize with the IP redundancy clients.
Active router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the current active Hot Standby router.
Standby router is	Value can be “local,” “unknown,” or an IP address. Address (and the expiration date of the address) of the “standby” router (the router that is next in line to be the Hot Standby router).
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Tracking	List of interfaces that are being tracked and their corresponding states. Based on the <b>standby track</b> command.
IP redundancy name is	Name of the IP redundancy service. The default name is derived from the interface and group number.

**Related Commands**

Command	Description
<b>standby authentication</b>	Configures an authentication string for HSRP.
<b>standby ip</b>	Activates HSRP.
<b>standby mac-address</b>	Specifies the virtual MAC address for the virtual router.
<b>standby mac-refresh</b>	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.
<b>standby preempt</b>	Configures HSRP preemption and preemption delay.
<b>standby priority</b>	Configures Hot Standby priority of potential standby routers.
<b>standby timers</b>	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
<b>standby track</b>	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
<b>standby use-bia</b>	Configures HSRP to use the BIA of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring).

# show standby delay

To display Hot Standby Router Protocol (HSRP) information about delay periods, use the **show standby delay** command in user EXEC or privileged EXEC mode.

**show standby delay** [*type number*]

<b>Syntax Description</b>	<i>type number</i> (Optional) Interface type and number for which output is displayed.
---------------------------	--

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2	This command was introduced.

**Examples** The following is sample output from the **show standby delay** command:

```
Router# show standby delay

Interface      Minimum Reload
Ethernet0/3    1           5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>standby delay</b> <b>minimum reload</b>	Delays the initialization of HSRP groups.

# show standby redirect

To display Internet Control Message Protocol (ICMP) redirect information on interfaces configured with the Hot Standby Router Protocol (HSRP), use the **show standby redirect** command in user EXEC or privileged EXEC mode.

**show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]

Syntax Description	
<i>ip-address</i>	(Optional) Router IP address.
<i>interface-type</i> <i>interface-number</i>	(Optional) Interface type and number for which output is displayed.
<b>active</b>	(Optional) Active HSRP routers on the subnet.
<b>passive</b>	(Optional) Passive HSRP routers on the subnet.
<b>timers</b>	(Optional) HSRP ICMP redirect timers.

Command Modes	
	User EXEC Privileged EXEC

Command History	Release	Modification
	12.2	This command was introduced.

**Examples** The following is sample output from the **show standby direct** command with no optional keywords:

Router# **show standby redirect**

```

Interface          Redirects Unknown   Adv    Holddown
Ethernet0/2        enabled  enabled   30     180
Ethernet0/3        enabled  disabled  30     180

Active             Hits    Interface      Group Virtual IP      Virtual MAC
10.19.0.7          0       Ethernet0/2    3     10.19.0.13       0000.0c07.ac03
local              0       Ethernet0/3    1     10.20.0.11       0000.0c07.ac01
local              0       Ethernet0/3    2     10.20.0.12       0000.0c07.ac02

Passive            Hits    Interface      Expires in
10.19.0.6          0       Ethernet0/2    151.800

```

[Table 40](#) describes the significant fields in the display.

**Table 40** *show standby redirects Field Descriptions*

Field	Description
Interface	Interface type and number for the interface.
Redirects	Indicates whether redirects are enabled or disabled on the interface.
Unknown	Indicates whether redirects to an unknown router are enabled or disabled on the interface.

**Table 40** *show standby redirects Field Descriptions*

Field	Description
Adv	Number indicating the passive router advertisement interval in seconds.
Holddown	Number indicating the passive router hold interval in seconds.
Active	Active HSRP routers on the subnet.
Hits	Number of address translations required for ICMP information.
Interface	Interface type and number for the interface on the active router.
Group	Hot standby group number.
Virtual IP	Virtual IP address of the active HSRP router.
Virtual MAC	Virtual MAC address of the active HSRP router.
Passive	Passive HSRP routers on the subnet.
Hits	Number of address translations required for ICMP information.
Interface	Interface type and number for the interface on the passive router.
Expires in	Time in seconds for a virtual IP to expire and the holddown time to apply for filtering routes to the standby router.

The following is sample output from the **show standby direct** command with a specific interface Ethernet 0/3:

```
Router# show standby redirect e0/3
```

```
Interface          Redirects Unknown  Adv    Holddown
Ethernet0/3        enabled  disabled  30     180

Active    Hits   Interface          Group Virtual IP    Virtual MAC
local     0     Ethernet0/3        1     10.20.0.11    0000.0c07.ac01
local     0     Ethernet0/3        2     10.20.0.12    0000.0c07.ac02
```

The following is sample output from the **show standby direct** command showing all active routers on interface Ethernet 0/3:

```
Router# show standby redirect e0/3 active
```

```
Active    Hits   Interface          Group Virtual IP    Virtual MAC
local     0     Ethernet0/3        1     10.20.0.11    0000.0c07.ac01
local     0     Ethernet0/3        2     10.20.0.12    0000.0c07.ac02
```

The following is sample output from the **show standby direct ip-address** command, where the IP address is the real IP address of the router:

```
Router# show standby redirect 10.19.0.7
```

```
Active    Hits   Interface          Group Virtual IP    Virtual MAC
10.19.0.7  0     Ethernet0/2        3     10.19.0.13    0000.0c07.ac03
```

**Related Commands**

Command	Description
<b>show standby</b>	Displays the HSRP information.
<b>standby redirects</b>	Enables ICMP redirect messages to be sent when HSRP is configured on an interface.

# show tcp statistics

To display TCP statistics, use the **show tcp statistics** command in user EXEC or privileged EXEC mode.

## show tcp statistics

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	11.3	This command was introduced.

**Examples** The following is sample output from the **show tcp statistics** command:

```
Router# show tcp statistics

Rcvd: 210 Total, 0 no port
      0 checksum error, 0 bad offset, 0 too short
      132 packets (26640 bytes) in sequence
      5 dup packets (502 bytes)
      0 partially dup packets (0 bytes)
      0 out-of-order packets (0 bytes)
      0 packets (0 bytes) with data after window
      0 packets after close
      0 window probe packets, 0 window update packets
      0 dup ack packets, 0 ack packets with unsend data
      69 ack packets (3044 bytes)
Sent: 175 Total, 0 urgent packets
      16 control packets (including 1 retransmitted)
      69 data packets (3029 bytes)
      0 data packets (0 bytes) retransmitted
      73 ack only packets (49 delayed)
      0 window probe packets, 17 window update packets
7 Connections initiated, 1 connections accepted, 8 connections established
8 Connections closed (including 0 dropped, 0 embryonic dropped)
1 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```

[Table 41](#) describes the significant fields shown in the display.

**Table 41** *show tcp statistics Field Descriptions*

Field	Description
Rcvd:	Statistics in this section refer to packets received by the router.
Total	Total number of TCP packets received.
no port	Number of packets received with no port.
checksum error	Number of packets received with checksum error.

**Table 41** *show tcp statistics Field Descriptions (continued)*

Field	Description
bad offset	Number of packets received with bad offset to data.
too short	Number of packets received that were too short.
packets in sequence	Number of data packets received in sequence.
dup packets	Number of duplicate packets received.
partially dup packets	Number of packets received with partially duplicated data.
out-of-order packets	Number of packets received out of order.
packets with data after window	Number of packets received with data that exceeded the window size of the receiver.
packets after close	Number of packets received after the connection was closed.
window probe packets	Number of window probe packets received.
window update packets	Number of window update packets received.
dup ack packets	Number of duplicate acknowledgment packets received.
ack packets with unsend data	Number of acknowledgment packets received with unsend data.
ack packets	Number of acknowledgment packets received.
Sent:	Statistics in this section refer to packets sent by the router.
Total	Total number of TCP packets sent.
urgent packets	Number of urgent packets sent.
control packets	Number of control packets (SYN, FIN, or RST) sent.
data packets	Number of data packets sent.
data packets retransmitted	Number of data packets re-sent.
ack only packets	Number of packets sent that are acknowledgments only.
window probe packets	Number of window probe packets sent.
window update packets	Number of window update packets sent.
Connections initiated	Number of connections initiated.
connections accepted	Number of connections accepted.
connections established	Number of connections established.
Connections closed	Number of connections closed.
Total rxmt timeout	Number of times the router tried to resend, but timed out.
connections dropped in rxmit timeout	Number of connections dropped in the resend timeout.
Keepalive timeout	Number of keepalive packets in the timeout.
keepalive probe	Number of keepalive probes.
Connections dropped in keepalive	Number of connections dropped in the keepalive.

**Related Commands**

Command	Description
<b>clear tcp statistics</b>	Clears TCP statistics.

# show time-range ipc

To display the statistics about the time-range interprocess communications (IPC) messages between the Route Processor and line card, use the **show time-range ipc** command in user EXEC or privileged EXEC mode.

## show time-range ipc

**Syntax Description** This command has no argument or keywords.

**Defaults** No default behavior or values.

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	12.2(2)T	This command was introduced.

**Usage Guidelines** The **debug time-range ipc** EXEC command must be enabled for the **show time-range ipc** command to display the time-range IPC message statistics.

**Examples** The following is sample output from the **show time-range ipc** command:

```
Router# show time-range ipc

RP Time range Updates Sent :3
RP Time range Deletes Sent :2
```

The display lists the number of time-range updates and time-range deletes sent by the Route Processor.

Related Commands	Command	Description
	<b>clear time-range ipc</b>	Clears the time-range IPC message statistics and counters between the Route Processor and the line card.
	<b>debug time-range ipc</b>	Enables debugging output for monitoring the time-range IPC messages between the Route Processor and the line card.



# show track

To display tracking information, use the **show track** command in privileged EXEC mode.

```
show track [[object-number / brief] / [interface [brief] | ip route [brief] | resolution | timers]
```

Syntax Description	
<i>object-number</i>	(Optional) Object number that represents the object to be tracked. Range is from 1 to 500.
<b>brief</b>	(Optional) Displays a single line of output.
<b>interface</b>	(Optional) Displays tracked interface objects. The <b>brief</b> keyword is optional and displays a single line of interface information.
<b>ip route</b>	(Optional) Displays tracked IP-route objects. The <b>brief</b> keyword is optional and displays a single line of route information. Range is from 1 to 500.
<b>resolution</b>	(Optional) Displays resolution of tracked parameters.
<b>timers</b>	(Optional) Displays polling interval timers.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.
	12.3(8)T	The output was enhanced to include the track-list objects.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines	
	Use this command to display information about objects that are tracked by the tracking process. When no keywords are specified, information for all objects is displayed.

Examples	
	The following example shows information about the state of IP routing on the interface that is being tracked:

```
Router# show track 1

Track 1
  Interface Ethernet0/2 ip routing
  IP routing is Down (no IP addr)
  1 change, last change 00:01:08
  Tracked by:
    HSRP Ethernet0/3 1
```

The following example shows information about the line-protocol state on the interface that is being tracked:

```
Router# show track 1

Track 1
  Interface Ethernet0/1 line-protocol
  Line protocol is Up
```

```

1 change, last change 00:00:05
Tracked by:
  HSRP Ethernet0/3 1

```

The following example shows information about the reachability of a route that is being tracked:

```

Router# show track 1

Track 1
IP route 10.16.0.0 255.255.0.0 reachability
Reachability is Up (RIP)
  1 change, last change 00:02:04
First-hop interface is Ethernet0/1
Tracked by:
  HSRP Ethernet0/3 1

```

The following example shows information about the threshold metric of a route that is being tracked:

```

Router# show track 1

Track 1
IP route 10.16.0.0 255.255.0.0 metric threshold
Metric threshold is Up (RIP/6/102)
  1 change, last change 00:00:08
Metric threshold down 255 up 254
First-hop interface is Ethernet0/1
Tracked by:
  HSRP Ethernet0/3 1

```

The following example shows the object type, the interval in which it is polled, and the time until the next poll:

```

Router# show track timers

Object type  Poll Interval  Time to next poll
interface      1             expired
ip route      30            29.364

```

Table 2 describes the significant fields shown in the displays.

**Table 2** *show track Field Descriptions*

Field	Description
Track	Object number that is tracked.
Interface Ethernet0/2 ip routing	Interface type, number, and object that is tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times the state of a tracked object has changed and the time (in hh:mm:ss) since the last change.
Tracked by	Client process that is tracking the object.
First-hop interface is	Displays the first-hop interface.
Object type	Object type that is being tracked.
Poll Interval	Interval (in seconds) in which the tracking process polls the object.
Time to next poll	Period of time until the next polling of the object.

The following output shows that there are two objects. Object 1 has been configured with a weight of 10 “down,” and object 2 has been configured with a weight of 20 “up.” Object 1 is down (expressed as 0/10) and object 2 is up. The total weight of the tracked list is 20 with a maximum of 30 (expressed as 20/30). The “up” threshold is 20, so the list is “up.”

```
Router# show track

Track 6
List threshold weight
Threshold weight is Up (20/30)
 1 change, last change 00:00:08
 object 1 Down (0/10)
 object 2 weight 20 Up (20/30)
Threshold weight down 10 up 20
Tracked by:
  HSRP Ethernet0/3 1
```

The following example shows information about the Boolean configuration:

```
Router# show track

Track 3
List boolean and
Boolean AND is Down
 1 change, last change 00:00:08
 object 1 not Up
 object 2 Down
Tracked by:
  HSRP Ethernet0/3 1
```

[Table 43](#) describes the significant fields shown in the displays.

**Table 43** *show track Field Descriptions*

Field	Description
Track	Object number that is tracked.
Boolean AND is Down	
1 change, last change	Number of times the state of a tracked object has changed and the time (in hh:mm:ss) since the last change.
Tracked by	Client process that is tracking the object; in this case, HSRP.

#### Related Commands

Command	Description
<b>track interface</b>	Configures an interface to be tracked and enters tracking configuration mode.
<b>track ip route</b>	Tracks the state of an IP route and enters tracking configuration mode.

# show vrrp

To display a brief or detailed status of one or all configured Virtual Router Redundancy Protocol (VRRP) groups on the router, use the **show vrrp** command in privileged EXEC mode.

**show vrrp** [**brief** | *group*]

Syntax Description	Parameter	Description
	<b>brief</b>	(Optional) Provides a summary view of the group information.
	<i>group</i>	(Optional) Virtual router group number of the group for which information is to be displayed. The group number is configured with the <b>vrrp ip</b> command.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(18)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(2)T	This command was enhanced to display the state of a tracked object.
	12.3(106)T	This command was enhanced to display MD5 authentication, key-strings, and time outs.

**Usage Guidelines** If no group is specified, all groups are displayed.

**Examples** The following is sample output for the **show vrrp** command:

```
Router# show vrrp

Ethernet1/0 - Group 1
State is Master
Virtual IP address is 10.2.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority 100
  Track object 1 state down decrement 15
Master Router is 10.2.0.1 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down interval is 9.609 sec

Ethernet1/0 - Group 2
State is Master
Virtual IP address is 10.0.0.20
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
```

```

Preemption is enabled
  min delay is 0.000 sec
Priority 95
Master Router is 10.0.0.1 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down interval is 3.628 sec

```

Table 44 describes the significant fields shown in the display.

**Table 44** show vrrp Field Descriptions

Field	Description
Ethernet1/0 - Group	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (master or backup).
Virtual IP address is	Virtual IP address for this group.
Virtual MAC address is	Virtual MAC address for this group.
Advertisement interval is	Interval at which the router will send VRRP advertisements when it is the master virtual router. This value is configured with the <b>vrrp timers advertise</b> command.
Preemption is	Indication of whether preemption is enabled or disabled.
Track object	Object number representing the object to be tracked.
state	State value (up or down) of the object being tracked.
decrement	Amount by which the priority of the router is decremented (or incremented) when the tracked object goes down (or comes back up).
Priority	Priority of the interface.
Master Router is	IP address of the current master virtual router.
priority is	Priority of the current master virtual router.
Master Advertisement interval is	Advertisement interval of the master virtual router.
Master Down interval is	Calculated time that the master virtual router can be down before the backup virtual router takes over.

The following is sample output from the **show vrrp** command with the **brief** keyword:

```
Router# show vrrp brief
```

```

Interface      Grp  Prio  Time   Own  Pre  State  Master addr  Group addr
Ethernet1/0    1    100   3609   P    P    Master  1.0.0.4      1.0.0.10
Ethernet1/0    2    105   3589   P    P    Master  1.0.0.4      1.0.0.20

```

Table 45 describes the significant fields shown in the display.

**Table 45** show vrrp brief Field Descriptions

Field	Description
Interface	Interface type and number.
Grp	VRRP group to which this interface belongs.
Prio	VRRP priority number for this group.

**Table 45** *show vrrp brief Field Descriptions*

Field	Description
Time	Calculated time that the master virtual router can be down before the backup virtual router takes over.
Own	IP address owner.
Pre	Preemption. P indicates that preemption is enabled. If this field is empty, preemption is disabled.
State	Role this interface plays within VRRP (master or backup).
Master addr	IP address of the master virtual router.
Group addr	IP address of the virtual router.

The following sample output shows the MD5 authentication, key string, and timeout value:

```
Router# show vrrp

Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority is 100
Authentication MD5, key-string "f00b4r", timeout 30 secs
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

See [Table 44](#) for descriptions of the significant fields in the output.

**Related Commands**

Command	Description
<b>vrrp ip</b>	Enables VRRP on an interface and identifies the IP address of the virtual router.

# show vrrp interface

To display the Virtual Router Redundancy Protocol (VRRP) groups and their status on a specified interface, use the **show vrrp interface** command in user EXEC or privileged EXEC mode.

**show vrrp interface** *type number* [**brief**]

Syntax Description	Parameter	Description
	<i>type</i>	Interface type.
	<i>number</i>	Interface number.
	<b>brief</b>	(Optional) Provides a summary view of the group information

Command Modes	Mode
	User EXEC Privileged EXEC

Command History	Release	Modification
	12.0(18)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Examples

The following is sample output from the **show vrrp interface** command:

```
Router# show vrrp interface ethernet 1/0

Ethernet1/0 - Group 1
State is Master
Virtual IP address is 10.2.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
min delay is 0.000 sec
Priority 100
Master Router is 10.2.0.1 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down interval is 9.609 sec

Ethernet1/0 - Group 2
State is Master
Virtual IP address is 10.0.0.20
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
Preemption is enabled
min delay is 0.000 sec
Priority 95
Master Router is 10.0.0.1 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down interval is 3.628 sec
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.



# standby authentication

To configure an authentication string for the Hot Standby Router Protocol (HSRP), use the **standby authentication** command in interface configuration mode. To delete an authentication string, use the **no** form of this command.

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

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

Syntax Description		
<i>group-number</i>	(Optional) Group number on the interface to which this authentication string applies.	
<b>text</b> <i>string</i>	Authentication string. It can be up to eight characters long. The default string is cisco.	
<b>md5</b>	Message Digest 5 (MD5) authentication.	
<b>key-string</b> <i>key</i>	Specifies the secret key for MD5 authentication. The key can contain up to 64 characters. We recommend using at least 16 characters.	
<b>0</b>	(Optional) Unencrypted key. If no prefix is specified, the text also is unencrypted.	
<b>7</b>	(Optional) Encrypted key.	
<b>timeout</b> <i>seconds</i>	(Optional) Duration in seconds that HSRP will accept message digests based on both the old and new keys.	
<b>key-chain</b> <i>name-of-chain</i>	Identifies a group of authentication keys.	

**Defaults** The default group number is 0. The default text authentication string is cisco.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.1	The <b>text</b> keyword was added.
	12.3(2)T	The <b>md5</b> keyword and associated parameters were added.

**Usage Guidelines** The authentication string is sent unencrypted in all HSRP messages when using the **standby authentication text** *string* option. The same authentication string must be configured on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and the Hot Standby timer values from other routers configured with HSRP.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

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

The **timeout seconds** is the duration that the HSRP group will accept message digests based on both the old and new keys. This allows time for configuration of all routers in a group with the new key. HSRP route flapping can be minimized by changing the keys on all the routers, provided that the active router is changed last. The active router should have its key string changed no later than one holdtime period, specified by the **standby timers** interface configuration command, after the non-active routers. This procedure ensures that the non-active routers do not time out the active router.

## Examples

The following example configures “company1” as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
interface ethernet 0
 standby 1 authentication text company1
```

The following example configures MD5 authentication using a key string named “345890”:

```
!
interface Ethernet0/1
 standby 1 ip 10.21.0.12
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-string 345890 timeout 30
```

The following example configures MD5 authentication using a key chain. HSRP queries the key chain “hsrp1” to obtain the current live key and key ID for the specified key chain:

```
key chain hsrp1
 key 1
 key-string 543210

interface Ethernet0/1
 standby 1 ip 10.21.0.10
 standby 1 priority 110
 standby 1 preempt
 standby 1 authentication md5 key-chain hsrp1
```

## Related Commands

Command	Description
<b>service password-encryption</b>	Encrypts passwords.
<b>standby timers</b>	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.

# standby delay minimum reload

To configure the delay period before the initialization of Hot Standby Router Protocol (HSRP) groups, use the **standby delay minimum reload** command in interface configuration mode. To disable the delay period, use the **no** form of this command.

**standby delay minimum** [*min-delay*] **reload** [*reload-delay*]

**no standby delay minimum** [*min-delay*] **reload** [*reload-delay*]

Syntax Description	<i>min-delay</i>	(Optional) Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events.
	<i>reload-delay</i>	(Optional) Time (in seconds) to delay after the router has reloaded. This delay period applies only to the first interface-up event after the router has reloaded.

**Defaults**

The default minimum delay is 1 second.  
The default reload delay is 5 seconds.

**Command Modes**

Interface configuration

Command History	Release	Modification
	12.2	This command was introduced.

**Usage Guidelines**

If the active router fails or is removed from the network, then the standby router will automatically become the new active router. If the former active router comes back online, you can control whether it takes over as the active router by using the **standby preempt** command.

However, in some cases, even if the **standby preempt** command is not configured, the former active router will resume the active role after it reloads and comes back online. Use the **standby delay minimum reload** command to set a delay period for HSRP group initialization. This command allows time for the packets to get through before the router resumes the active role.

We recommend that you use the **standby delay minimum reload** command if the **standby timers** command is configured in milliseconds or if HSRP is configured on a VLAN interface of a switch.

In most configurations, the default values provide sufficient time for the packets to get through and configuring longer delay values is not necessary.

The delay will be cancelled if an HSRP packet is received on an interface.

**Examples**

The following example sets the minimum delay period to 30 seconds and the delay period after the first reload to 120 seconds:

```
interface ethernet 0
 ip address 10.20.0.7 255.255.0.0
```

```
standby delay minimum 30 reload 120
standby 3 ip 10.20.0.21
standby 3 timers msec 300 msec 700
standby 3 priority 100
```

**Related Commands**

Command	Description
<b>show standby delay</b>	Displays HSRP information about delay periods.
<b>standby preempt</b>	Configures the HSRP preemption and preemption delay.
<b>standby timers</b>	Configures the time between hello packets and the time before other routers declare the active HSRP or standby router to be down.

# standby ip

To activate the Hot Standby Router Protocol (HSRP), use the **standby ip** command in interface configuration mode. To disable HSRP, use the **no** form of this command.

**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

**no standby** [*group-number*] **ip** [*ip-address*]

Syntax Description	
<i>group-number</i>	(Optional) Group number on the interface for which HSRP is being activated. The default is 0. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2.
<i>ip-address</i>	(Optional) IP address of the Hot Standby router interface.
<b>secondary</b>	(Optional) Indicates the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

**Defaults** The default group number is 0.  
HSRP is disabled by default.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The <i>group-number</i> argument was added.
	11.1	The <b>secondary</b> keyword was added.
	12.3(4)T	The group number range was expanded for HSRP version 2.

**Usage Guidelines** The **standby ip** command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the designated address is learned through the standby function. For HSRP to elect a designated router, at least one router on the cable must have been configured with, or have learned, the designated address. Configuration of the designated address on the active router always overrides a designated address that is currently in use.

When the **standby ip** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). If the Hot Standby state of the interface is active, proxy ARP requests are answered using the MAC address of the Hot Standby group. If the interface is in a different state, proxy ARP responses are suppressed.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

HSRP version 2 permits an expanded group number range from 0 to 4095. The increased group number range does not imply that an interface can, or should, support that many HSRP groups. The expanded group number range was changed to allow the group number to match the VLAN number on subinterfaces.

---

**Examples**

The following example activates HSRP for group 1 on Ethernet interface 0. The IP address used by the Hot Standby group will be learned using HSRP.

```
interface ethernet 0
  standby 1 ip
```

In the following example, all three virtual IP addresses appear in the ARP table using the same (single) virtual MAC address. All three virtual IP addresses are using the same HSRP group (group 0).

```
ip address 10.1.1.1 255.255.255.0
ip address 10.2.2.2 255.255.255.0 secondary
ip address 10.3.3.3 255.255.255.0 secondary
ip address 10.4.4.4 255.255.255.0 secondary
standby ip 10.1.1.254
standby ip 10.2.2.254 secondary
standby ip 10.3.3.254 secondary
```

# standby mac-address

To specify a virtual MAC address for the Hot Standby Router Protocol (HSRP), use the **standby mac-address** command in interface configuration mode. To revert to the standard virtual MAC address (0000.0C07.ACxy), use the **no** form of this command.

**standby** [*group-number*] **mac-address** *mac-address*

**no standby** [*group-number*] **mac-address**

## Syntax Description

<i>group-number</i>	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
<i>mac-address</i>	MAC address.

## Defaults

If this command is not configured, and the **standby use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.ACxy, where xy is the group number in hexadecimal. This address is specified in RFC 2281, *Cisco Hot Standby Router Protocol (HSRP)*.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.2	This command was introduced.

## Usage Guidelines

This command cannot be used on a Token Ring interface.

HSRP is used to help end stations locate the first-hop gateway for IP routing. The end stations are configured with a default gateway. However, HSRP can provide first-hop redundancy for other protocols. Some protocols, such as Advanced Peer-to-Peer Networking (APPN), use the MAC address to identify the first hop for routing purposes. In this case, it is often necessary to be able to specify the virtual MAC address; the virtual IP address is unimportant for these protocols. Use the **standby mac-address** command to specify the virtual MAC address.

The MAC address specified is used as the virtual MAC address when the router is active.

This command is intended for certain APPN configurations. The parallel terms are shown in [Table 46](#).

**Table 46** Parallel Terms Between APPN and IP

APPN	IP
End node	Host
Network node	Router or gateway

In an APPN network, an end node is typically configured with the MAC address of the adjacent network node. Use the **standby mac-address** command in the routers to set the virtual MAC address to the value used in the end nodes.

---

**Examples**

If the end nodes are configured to use 4000.1000.1060 as the MAC address of the network node, the following example shows the command used to configure HSRP group 1 with the virtual MAC address:

```
standby 1 mac-address 4000.1000.1060
```

---

**Related Commands**

Command	Description
<b>show standby</b>	Displays HSRP information.
<b>standby use-bia</b>	Configures HSRP to use the burned-in address of the interface as its virtual MAC address.

---



# standby mac-refresh

To change the interval at which packets are sent to refresh the MAC cache when the Hot Standby Router Protocol (HSRP) is running over FDDI, use the **standby mac-refresh** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**standby mac-refresh** *seconds*

**no standby mac-refresh**

<b>Syntax Description</b>	<i>seconds</i>	Number of seconds in the interval at which a packet is sent to refresh the MAC cache. The maximum value is 255 seconds. The default is 10 seconds.
---------------------------	----------------	--

<b>Defaults</b>	Seconds: 10 seconds.
-----------------	----------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0	This command was introduced.

<b>Usage Guidelines</b>	This command applies to HSRP running over FDDI only. Packets are sent every 10 seconds to refresh the MAC cache on learning bridges or switches. By default, the MAC cache entries age out in 300 seconds (5 minutes).
-------------------------	--

All other routers participating in HSRP on the FDDI ring receive the refresh packets, although the packets are intended only for the learning bridge or switch. Use this command to change the interval. Set the interval to 0 if you want to prevent refresh packets (if you have FDDI but do not have a learning bridge or switch).

<b>Examples</b>	The following example changes the MAC refresh interval to 100 seconds. Therefore, a learning bridge would need to miss three packets before the entry ages out.
-----------------	---

```
standby mac-refresh 100
```

# standby name

To configure the name of the standby group, use the **standby name** command in interface configuration mode. To disable the name, use the **no** form of this command.

**standby name** *group-name*

**no standby name** *group-name*

Syntax Description	<i>group-name</i>	Specifies the name of the standby group.
--------------------	-------------------	--

Defaults	The Hot Standby Router Protocol (HSRP) is disabled.
----------	---

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

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

Usage Guidelines	The name specifies the HSRP group used.
------------------	---

Examples	The following example specifies the standby name as SanJoseHA:
----------	--

```
interface ethernet0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
 standby preempt delay sync 100
 standby priority 110
```

Related Commands	Command	Description
	<b>ip mobile home-agent redundancy</b>	Configures the home agent for redundancy.

# standby preempt

To configure Hot Standby Router Protocol (HSRP) preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

```
standby [group-number] preempt [delay{minimum delay | reload delay | sync delay}]
```

```
no standby [group-number] preempt [delay{minimum delay | reload delay | sync delay}]
```

## Syntax Description

<i>group-number</i>	(Optional) Group number on the interface to which the other arguments in this command apply.
<b>delay</b>	(Optional) Required if either the <b>minimum</b> , <b>reload</b> , or <b>sync</b> keywords are specified.
<b>minimum</b> <i>delay</i>	(Optional) Specifies the minimum delay period in <i>delay</i> seconds. The <i>delay</i> argument causes the local router to postpone taking over the active role for <i>delay</i> (minimum) seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
<b>reload</b> <i>delay</i>	(Optional) Specifies the preemption delay after a reload only.
<b>sync</b> <i>delay</i>	(Optional) Specifies the maximum synchronization period in <i>delay</i> seconds.

## Defaults

The default group number is 0.  
The default delay is 0 seconds; if the router wants to preempt, it will do so immediately.  
By default, the router that comes up later becomes the standby.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.3	This command was introduced.
12.0(2)T	The <b>minimum</b> and <b>sync</b> keywords were added.
12.2	The behavior of the command changed such that <b>standby preempt</b> and <b>standby priority</b> must be entered as separate commands.
12.2	The <b>reload</b> keyword was added.

## Usage Guidelines

When this command is configured, the router is configured to preempt, which means that when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router. If preemption is not configured, the local router assumes control as the active router only if it receives information indicating no router is in the active state (acting as the designated router).

When a router first comes up, it does not have a complete routing table. If it is configured to preempt, it will become the active router, yet it is unable to provide adequate routing services. Solve this problem by configuring a delay before the preempting router actually preempts the currently active router.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

IP redundancy clients can prevent preemption from taking place. The **standby preempt delay sync** *delay* command specifies a maximum number of seconds to allow IP redundancy clients to prevent preemption. When this expires, then preemption takes place regardless of the state of the IP redundancy clients.

The **standby preempt delay reload** *delay* command allows preemption to occur only after a router reloads. This provides stabilization of the router at startup. After this initial delay at startup, the operation returns to the default behavior.

The **no standby preempt delay** command will disable the preemption delay but preemption will remain enabled. The **no standby preempt delay minimum** *delay* command will disable the minimum delay but leave any synchronization delay if it was configured.

---

## Examples

In the following example, the router will wait for 300 seconds (5 minutes) before attempting to become the active router:

```
interface ethernet 0
 standby ip 172.19.108.254
 standby preempt delay minimum 300
```

# standby priority

To configure Hot Standby Router Protocol (HSRP) priority, use the **standby priority** command in interface configuration mode. To restore the default values, use the **no** form of this command.

**standby** [*group-number*] **priority** *priority*

**no standby** [*group-number*] **priority** *priority*

Syntax Description		
<i>group-number</i>	(Optional) Group number on the interface to which the other arguments in this command apply. The default group number is 0.	
<i>priority</i>	Priority value that prioritizes a potential Hot Standby router. The range is from 1 to 255, where 1 denotes the lowest priority and 255 denotes the highest priority. The default priority value is 100. The router in the HSRP group with the highest priority value becomes the active router.	

Defaults	
	The default group number is 0. The default priority is 100.

Command Modes	
	Interface configuration

Command History	Release	Modification
	11.3	This command was introduced.
	12.2	The behavior of the command changed such that <b>standby preempt</b> and <b>standby priority</b> must be entered as separate commands.

Usage Guidelines	
	When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.
	The assigned priority is used to help select the active and standby routers. Assuming that preemption is enabled, the router with the highest priority becomes the designated active router. In case of ties, the primary IP addresses are compared, and the higher IP address has priority.
	Note that the priority of the device can change dynamically if an interface is configured with the <b>standby track</b> command and another interface on the router goes down.

Examples	
	In the following example, the router has a priority of 120 (higher than the default value):
	<pre>interface ethernet 0  standby ip 172.19.108.254  standby priority 120  standby preempt delay 300</pre>

Related Commands	Command	Description
	<b>standby track</b>	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

# standby redirects

To enable Hot Standby Router Protocol (HSRP) filtering of Internet Control Message Protocol (ICMP) redirect messages, use the **standby redirects** command in interface configuration mode. To disable the HSRP filtering of ICMP redirect messages, use the **no** form of this command.

**standby redirects** [**enable** | **disable**] [**timers** *advertisement holddown*] [**unknown**]

**no standby redirects** [**unknown**]

Syntax Description	enable	(Optional) Allows the filtering of ICMP redirect messages on interfaces configured with HSRP, where the next hop IP address may be changed to an HSRP virtual IP address.
	<b>disable</b>	(Optional) Disables the filtering of ICMP redirect messages on interfaces configured with HSRP.
	<b>timers</b>	(Optional) Adjusts HSRP router advertisement timers.
	<i>advertisement</i>	(Optional) HSRP Router advertisement interval in seconds. This is an integer from 10 to 180. The default is 60 seconds.
	<i>holddown</i>	(Optional) HSRP router holddown interval in seconds. This is an integer from 61 to 3600. The default is 180 seconds.
	<b>unknown</b>	(Optional) Allows sending of ICMP packets when the next hop IP address contained in the packet is unknown in the HSRP table of real IP addresses and active virtual IP addresses. The <b>no standby redirect unknown</b> command stops the redirects from being sent.

**Defaults** HSRP filtering of ICMP redirect messages is enabled if HSRP is configured on an interface.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2	The following keywords and arguments were added to the command: <ul style="list-style-type: none"> <li>• <b>timers</b> <i>advertisement holdtime</i></li> <li>• <b>unknown</b></li> </ul>

**Usage Guidelines** The **standby redirects** command can be configured globally or on a per-interface basis. When HSRP is first configured on an interface, the setting for that interface will inherit the global value. If the filtering of ICMP redirects is explicitly disabled on an interface, then the global command cannot reenable this functionality.

The **no standby redirects** command is the same as the **standby redirects disable** command. However, it is not desirable to save the **no** form of this command to NVRAM. Because the command is enabled by default, it is preferable to use the **standby redirects disable** command to disable the functionality.

With the **standby redirects** command enabled, the real IP address of a router can be replaced with a virtual IP address in the next hop address or gateway field of the redirect packet. HSRP looks up the next hop IP address in its table of real IP addresses versus virtual IP addresses. If HSRP does not find a match, the HSRP router allows the redirect packet to go out unchanged. The host HSRP router is redirected to a router that is unknown, that is, a router with no active HSRP groups. You can specify the **no standby redirects unknown** command to stop these redirects from being sent.

---

**Examples**

The following example shows how to allow HSRP to filter ICMP redirect messages on interface Ethernet 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# standby redirects
Router(config-if)# standby 1 ip 10.0.0.11
```

The following example shows how to change the HSRP router advertisement interval to 90 seconds and the holddown timer to 270 seconds on interface Ethernet 0:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# standby redirects timers 90 270
Router(config-if)# standby 1 ip 10.0.0.11
```

---

**Related Commands**

Command	Description
<b>show standby</b>	Displays the HSRP information.
<b>show standby redirect</b>	Displays ICMP redirect information on interfaces configured with the HSRP.



## standby timers

To configure the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down, use the **standby timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

**no standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*

Syntax Description	
<i>group-number</i>	(Optional) Group number on the interface to which the timers apply. The default is 0.
<b>msec</b>	(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
<i>hellotime</i>	Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the <b>msec</b> option is specified, hello interval is in milliseconds. This is an integer from 15 to 999.
<i>holdtime</i>	Time (in seconds) before the active or standby router is declared to be down. This is an integer from <i>x</i> to 255. The default is 10 seconds. If the <b>msec</b> option is specified, <i>holdtime</i> is in milliseconds. This is an integer from <i>y</i> to 3000.
	Where:
	<ul style="list-style-type: none"> <li><i>x</i> is the <i>hellotime</i> + 50 milliseconds, then rounded up to the nearest 1 second</li> <li><i>y</i> is greater than or equal to 3 times the <i>hellotime</i> and is not less than 50 milliseconds.</li> </ul>

Defaults	
	The default group number is 0.
	The default hello interval is 3 seconds.
	The default hold time is 10 seconds.

Command Modes	
	Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	11.2	The <b>msec</b> keyword was added.
	12.2	The minimum values of <i>hellotime</i> and <i>holdtime</i> in milliseconds changed.

Usage Guidelines	
	The <b>standby timers</b> command configures the time between standby hello packets and the time before other routers declare the active or standby router to be down. Routers or access servers on which timer values are not configured can learn timer values from the active or standby router. The timers configured on the active router always override any other timer settings. All routers in a Hot Standby group should use the same timer values. Normally, holdtime is greater than or equal to 3 times the value of hellotime.

The range of values for holdtime force the holdtime to be greater than the hellotime. If the timer values are specified in milliseconds, the holdtime is required to be at least three times the hellotime value and not less than 50 milliseconds.

Some HSRP state flapping can occasionally occur if the holdtime is set to less than 250 milliseconds, and the processor is busy. It is recommended that holdtime values less than 250 milliseconds be used on Cisco 7200 platforms or better, and on Fast-Ethernet or FDDI interfaces or better. Setting the **process-max-time** command to a suitable value may also help with flapping.

The value of the standby timer will not be learned through HSRP hellos if it is less than 1 second.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

---

## Examples

The following example sets, for group number 1 on Ethernet interface 0, the time between hello packets to 5 seconds, and the time after which a router is considered to be down to 15 seconds:

```
interface ethernet 0
 standby 1 ip
 standby 1 timers 5 15
```

The following example sets, for the Hot Router interface located at 172.19.10.1 on Ethernet interface 0, the time between hello packets to 300 milliseconds, and the time after which a router is considered to be down to 900 milliseconds:

```
interface ethernet 0
 standby ip 172.19.10.1
 standby timers msec 300 msec 900
```

The following example sets, for the Hot Router interface located at 172.18.10.1 on Ethernet interface 0, the time between hello packets to 15 milliseconds, and the time after which a router is considered to be down to 50 milliseconds. Note that the holdtime is larger than three times the hellotime because the minimum holdtime value in milliseconds is 50.

```
interface ethernet 0
 standby ip 172.18.10.1
 standby timers msec 15 msec 50
```

# standby track

To configure the Hot Standby Router Protocol (HSRP) to track an object and change the Hot Standby priority on the basis of the state of the object, use the **standby track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

## Cisco IOS Release 12.2(15)T and Later Releases

```
standby [group-number] track object-number [decrement [priority-decrement]]
no standby [group-number] track object-number [decrement [priority-decrement]]
```

## Cisco IOS Release 12.2(13)T and Earlier Releases

```
standby [group-number] track interface-type interface-number [interface-priority]
no standby [group-number] track interface-type interface-number [interface-priority]
```

Syntax Description		
<i>group-number</i>	(Optional) Group number to which the tracking applies.	
<i>object-number</i>	Object number that represents the object to be tracked. Range is from 1 to 500. Default is 1.	
<b>decrement</b> <i>priority-decrement</i>	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). Range is from 1 to 255. Default is 10.	
<i>interface-type</i>	Interface type (combined with interface number) that will be tracked.	
<i>interface-number</i>	Interface number (combined with interface type) that will be tracked.	
<i>interface-priority</i>	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). Range is from 0 to 255. Default is 10.	

**Defaults** There is no tracking.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.
	12.2(15)T	This command was enhanced to allow HSRP to track objects other than the interface line-protocol state.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

---

## Usage Guidelines

This command ties the Hot Standby priority of the router to the availability of its tracked objects. Use the **track interface** or **track ip route** global configuration commands to track an interface object or an IP-route object. The HSRP client can register its interest in the tracking process by using the **standby track** command and take action when the object changes.

When a tracked object goes down, the Hot Standby priority decreases by 10. If an object is not tracked, its state changes do not affect the Hot Standby priority. For each object configured for Hot Standby, you can configure a separate list of objects to be tracked.

The optional *priority* argument specifies how much to decrement the Hot Standby priority when a tracked object goes down. When the tracked object comes back up, the priority is incremented by the same amount.

When multiple tracked objects are down, the decrements are cumulative, whether configured with *priority* values or not.

Use the **no standby group-number track** command to delete all tracking configuration for a group.

When group number 0 is used, no group number is written to NVRAM, providing backward compatibility.

The **standby track** command syntax prior to Cisco IOS Release 12.2(15)T is still supported. Using the older form of the command syntax will cause a tracked object to be created in the new tracking process. This tracking information can be displayed using the **show track** command.

---

## Examples

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0. HSRP on Ethernet interface 0/0 then registers with the tracking process to be informed of any changes to the IP-routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, the priority of the HSRP group is reduced by 10.

If both serial interfaces are operational, Router A will be the HSRP active router because it has the higher priority. However, if IP routing on serial interface 1/0 in Router A fails, the HSRP group priority will be reduced and Router B will take over as the active router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Router A Configuration

```
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
 ip address 10.1.0.21 255.255.0.0
 standby 1 preempt
 standby 1 ip 10.1.0.1
 standby 1 priority 105
 standby 1 track 100 decrement 10
```

### Router B Configuration

```
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
 ip address 10.1.0.22 255.255.0.0
 standby 1 preempt
 standby 1 ip 10.1.0.1
 standby 1 priority 11
 standby 1 track 100 decrement 10
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
show track	Displays HSRP information.
<b>standby preempt</b>	Configures HSRP preemption and preemption delay.
<b>standby priority</b>	Configures Hot Standby priority of potential standby routers.
<b>track interface</b>	Configures an interface to be tracked and enters tracking configuration mode.
<b>track ip route</b>	Tracks the state of an IP route and enters tracking configuration mode.

# standby use-bia

To configure the Hot Standby Router Protocol (HSRP) to use the burned-in address of the interface as its virtual MAC address, instead of the preassigned MAC address (on Ethernet and FDDI) or the functional address (on Token Ring), use the **standby use-bia** command in interface configuration mode. To restore the default virtual MAC address, use the **no** form of this command.

**standby use-bia** [**scope interface**]

**no standby use-bia**

<b>Syntax Description</b>	<b>scope interface</b> (Optional) Specifies that this command is configured just for the subinterface on which it was entered, instead of the major interface.
---------------------------	--

<b>Defaults</b>	HSRP uses the preassigned MAC address on Ethernet and FDDI, or the functional address on Token Ring.
-----------------	--

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.2	This command was introduced.
	12.1	The behavior was modified to allow multiple standby groups to be configured for an interface configured with this command

<b>Usage Guidelines</b>	<p>For an interface with this command configured, multiple standby group can be configured. Hosts on the interface must have a default gateway configured. We recommend that you set the <b>no ip proxy-arp</b> command on the interface. It is desirable to configure the <b>standby use-bia</b> command on a Token Ring interface if there are devices that reject ARP replies with source hardware addresses set to a functional address.</p> <p>When HSRP runs on a multiple-ring, source-routed bridging environment and the HRSP routers reside on different rings, configuring the <b>standby use-bia</b> command can prevent confusion about the routing information field (RFI).</p> <p>Without the <b>scope interface</b> keywords, the <b>standby use-bia</b> command applies to all subinterfaces on the major interface. The <b>standby use-bia</b> command may not be configured both with and without the <b>scope interface</b> keywords at the same time.</p>
-------------------------	--

<b>Examples</b>	In the following example, the burned-in address of Token Ring interface 4/0 will be the virtual MAC address mapped to the virtual IP address:
-----------------	---

```
interface token4/0
 standby use-bia
```

# standby version

To change the version of the Hot Standby Router Protocol (HSRP), use the **standby version** command in interface configuration mode. To change to the default version, use the **no** form of this command.

**standby version { 1 | 2 }**

**no standby version**

Syntax Description	1	Specifies HSRP version 1.
	2	Specifies HSRP version 2.

**Defaults** HSRP version 1 is the default HSRP version.

**Command Modes** Interface configuration

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

**Usage Guidelines** HSRP version 2 addresses limitations of HSRP version 1 by providing an expanded group number range of 0 to 4095.

HSRP version 2 does not interoperate with HSRP version 1. An interface cannot operate both version 1 and version 2 because both versions are mutually exclusive. However, the different versions can be run on different physical interfaces of the same router. The group number range is from 0 to 255 for HSRP version 1 and from 0 to 4095 for HSRP version 2. You cannot change from version 2 to version 1 if you have configured groups above 255. Use the **no standby version** command to set the HSRP version to the default version, version 1.

If an HSRP version is changed, each group will reinitialize because it now has a new virtual MAC address.

**Examples** The following example shows how to configure HSRP version 2 on an interface with a group number of 500:

```
!
interface vlan500
 standby version 2
 standby 500 ip 172.20.100.10
 standby 500 priority 110
 standby 500 preempt
 standby 500 timers 5 15
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show standby</b>	Displays HSRP information.

---



# start-forwarding-agent

To start the forwarding agent, use the **start-forwarding-agent** command in CASA-port configuration mode.

```
start-forwarding-agent port-number [password [timeout]]
```

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 initial number of affinities is 5000.  
The default maximum number of affinities is 30,000.

**Command Modes** CASA-port configuration

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

**Usage Guidelines**

The forwarding agent must be started before you can configure any port information for the forwarding agent.

**Examples**

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

```
start-forwarding-agent 1637
```

Related Commands	Command	Description
	<b>forwarding-agent</b>	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.

# sticky

To assign all connections from a client to the same real server, use the **sticky** command in virtual server configuration mode. To remove the client/server coupling, use the **no sticky** form of this command.

**sticky** *duration* [**group** *group-id*]

**no sticky**

Syntax Description		
	<i>duration</i>	Sticky timer duration (in seconds). Valid values range from 0 to 65535.
	<b>group</b>	(Optional) Places the virtual server in a sticky group, for coupling of services.
	<i>group-id</i>	(Optional) Number identifying the sticky group to which the virtual server belongs. Valid values range from 0 to 255.

## Defaults

Sticky connections are not tracked.

Virtual servers are not associated with any groups.

## 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.

## Usage Guidelines

The last real server that was used for a connection from a client is stored for the set *duration* seconds. If a new connection from the client to the virtual server is initiated during that time, the same real server that was used for the previous connection is chosen for the new connection. If two virtual servers are placed in the same group, coincident connection requests for those services from the same IP address are handled by the same real server.

## Examples

The following example specifies that if a subsequent request from a client for a virtual server is made within 60 seconds of the previous request, then the same real server is used for the connection. This example also places the virtual server in group 10.

```
ip slb vserver VS1
sticky 60 group 10
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip slb sticky</b>	Displays information about the virtual server or firewall farm sticky configuration.
<b>show ip slb vservers</b>	Displays information about the virtual servers.
<b>virtual</b>	Configures the virtual server attributes.

# subnet prefix-length

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

**subnet prefix-length** *prefix-length*

**no subnet prefix-length** *prefix-length*

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

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(15)T	This command was introduced.

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

## Configuring Global Subnet Pools

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

## Configuring VPN Subnet Pools

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

### Configuring VPN Subnet Pools for VPN clients with VPN IDs

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

## Examples

### Global Configuration Example

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

```
Router(config)# ip dhcp pool GLOBAL-POOL
Router(dhcp-config)# network 10.0.0.0 255.255.255.0
Router(dhcp-config)# subnet prefix-length 24
!
```

### VPN Configuration Example

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

```
Router(config)# ip dhcp pool VRF-POOL
Router(dhcp-config)# vrf RED
Router(dhcp-config)# network 172.16.0.0 /16
Router(dhcp-config)# subnet prefix-length 26
!
```

### VPN ID Configuration Example

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

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target both 100:1
Router(config-vrf)# vpn id 1234:123456
Router(config-vrf)# exit
Router(config)# ip dhcp pool VPN-POOL
Router(dhcp-config)# vrf RED
Router(dhcp-config)# network 192.168.0.0 /24
Router(dhcp-config)# subnet prefix-length /27
Router(dhcp-config)# exit
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ip dhcp database</b>	Configures a Cisco IOS DHCP server to save automatic bindings on a remote host called a database agent.
<b>ip dhcp pool</b>	Enables the IP address of an interface to be automatically configured when a DHCP pool is populated with a subnet from IPCP negotiation.
<b>network (DHCP)</b>	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
<b>show ip dhcp pool</b>	Displays information about the DHCP pools.

# synguard

To limit the rate of TCP SYNs handled by a virtual server to prevent an SYN flood Denial-of-Service attack, use the **synguard** command in virtual server configuration mode. To remove the threshold, use the **no** form of this command.

```
synguard syn-count [interval]
```

```
no synguard
```

Syntax Description		
	<i>syn-count</i>	Number of unanswered SYNs that are allowed to be outstanding to a virtual server. Valid values range from 0 (off) to 4294967295. The default is 0.
	<i>interval</i>	(Optional) Interval (in milliseconds) for SYN threshold monitoring. Valid values range from 50 to 5000. The default is 100 ms.

Defaults	
	The default SYN count is 0 (off).
	The default interval is 100 ms.

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.

Examples	
	The following example sets the threshold of unanswered SYNs to 50:
	<pre>ip slb vserver PUBLIC_HTTP synguard 50</pre>

Related Commands	Command	Description
	<b>show ip slb vservers</b>	Displays information about the virtual servers.
	<b>virtual</b>	Configures the virtual server attributes.

# term ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format** command in EXEC configuration mode. To restore the default display format, use the **no** form of this command.

**term ip netmask-format** { **bitcount** | **decimal** | **hexadecimal** }

**no term ip netmask-format** [**bitcount** | **decimal** | **hexadecimal**]

## Syntax Description

<b>bitcount</b>	Number of bits in the netmask.
<b>decimal</b>	Netmask dotted decimal notation.
<b>hexadecimal</b>	Netmask hexadecimal format.

## Defaults

Netmasks are displayed in dotted decimal format.

## Command Modes

EXEC

## Command History

Release	Modification
10.3	This command was introduced.

## Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This range of IP addresses is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.55 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.55/24.

## Examples

The following example specifies that network masks for the session be displayed in bitcount notation in the output of **show** commands:

```
term ip netmask-format bitcount
```



# threshold metric

To set a threshold metric other than the default value, use the **threshold metric** command in tracking configuration mode. To disable the threshold metric, use the **no** form of this command.

**threshold metric** {*up number* | *down number*}

**no threshold metric** {*up number* | *down number*}

Syntax Description	up	down
	Specifies the up threshold. The state is up if the scaled metric for that route is less than or equal to the up threshold. The default up threshold is 254.	Specifies the down threshold. The state is down if the scaled metric for that route is greater than or equal to the down threshold. The default down threshold is 255.
	<i>number</i>	Threshold value. Range is from 0 to 255.

**Defaults** No threshold is configured.

**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 only to IP-route threshold metric objects tracked by the **track ip route metric threshold** global configuration command.

The default up and down threshold values are 254 and 255, respectively. With these values, IP-route threshold tracking gives the same result as IP-route reachability tracking.

**Examples** In the following example, the tracking process is tracking the IP-route threshold metric. The metric default value is changed to 16 for the up threshold and to 20 for the down threshold.

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

Related Commands	Command	Description
	<b>track ip route</b>	Tracks the state of IP routing and enters tracking configuration mode.

# threshold percentage

To set a threshold percentage for a tracked object in a list of objects, use the **threshold percentage** command in tracking configuration mode. To disable the threshold percentage, use the **no** form of this command.

**threshold percentage** {**up** *number* | **down** *number*}

**no threshold percentage** {**up** *number* | **down** *number*}

## Syntax Description

<b>up</b>	Specifies the up threshold.
<b>down</b>	Specifies the down threshold.
<i>number</i>	Threshold value. Range is from 0 to 100.

## Defaults

No threshold percentage is configured.

## 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.

## Usage Guidelines

When you configure a tracked list using the **track *object-number* list** command, there are two keywords available: **boolean** and **threshold**. If you specify the **threshold** keyword, you can specify either the **percentage** or **weight** keywords. If you specify the **percentage** keyword, then the **weight** keyword is unavailable. If you specify the **weight** keyword, then the **percentage** keyword is unavailable.

You should configure the “up” percentage first. The valid range is from 1 to 100. The down percentage depends on what you have configured for up. For example, if you configure 50 percent for up, you will see a range from 0 to 49 percent for down.

## Examples

In the following example, the tracked list 11 is configured to measure the threshold using an “up” percentage of 50 and a “down” percentage of 32.

```
track 11 list threshold percentage
  object 1
  object 2
  threshold percentage up 50 down 32
```

## Related Commands

Command	Description
<b>threshold weight</b>	Sets a threshold weight for a tracked object in a list of objects.

# threshold weight

To set a threshold weight for a tracked object in a list of objects, use the **threshold weight** command in tracking configuration mode. To disable the threshold weight, use the **no** form of this command.

**threshold weight** { **up** *number* | **down** *number* }

**no threshold weight** { **up** *number* | **down** *number* }

Syntax Description	Parameter	Description
	<b>up</b>	Specifies the up threshold.
	<b>down</b>	Specifies the down threshold.
	<i>number</i>	Threshold value. Range is from 1 to 255.

**Defaults** No threshold weight is configured.

**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.

**Usage Guidelines** When you configure a tracked list of objects using the **track *object-number* list** command, there are two keywords available: **boolean** and **threshold**. If you specify the **threshold** keyword, you can specify either the **percentage** or **weight** keywords. If you specify the **weight** keyword, then the **percentage** keyword is unavailable. If you specify the **percentage** keyword, then the **weight** keyword is unavailable. You should configure the “up” weight first. The valid range is from 1 to 255. The available “down” weight depends on what you have configured for the “up” weight. For example, if you configure 25 for up, you will see a range from 0 to 24 for down.

**Examples** In the following example, the tracked list 12 is configured to measure a threshold using a specified weight.

```
track 12 list threshold weight
  object 1
  object 2
  threshold weight up 35 down 22
```

Related Commands	Command	Description
	<b>threshold percentage</b>	Sets a threshold percentage for a tracked object in a list of objects

# track interface

To configure an interface to be tracked and to enter tracking configuration mode, use the **track interface** command in global configuration mode. To remove the tracking, use the **no** form of this command.

**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

**no track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}

Syntax Description		
	<i>object-number</i>	Object number that represents the interface to be tracked. Range is from 1 to 500.
	<i>type number</i>	Interface type and number to be tracked. No space is required between the values.
	<b>line-protocol</b>	Tracks the state of the interface line protocol.
	<b>ip routing</b>	Tracks whether IP routing is enabled, whether an IP address is configured on the interface, and whether the interface state is up, before reporting to the tracking client that the interface is up.

**Defaults** No interface is tracked.

**Command Modes** Global 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 reports a state value to clients. An IP-routing object is considered up when the following criteria exist:

- IP routing is enabled and active on the interface.
- The interface line-protocol state is up.
- The interface IP address is known. The IP address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.

Interface IP routing will go down when one of the following criteria exist:

- IP routing is disabled globally.
- The interface line-protocol state is down.
- The interface IP address is unknown. The IP address is not configured or received through DHCP or IPCP negotiation.

Tracking the IP-routing state of an interface using the **track interface ip routing** command can be more useful in some situations than just tracking the line-protocol state using the **track interface line-protocol** command, especially on interfaces for which IP addresses are negotiated. For example, on a serial interface that uses the Point-to-Point Protocol (PPP), the line protocol could be up [link control protocol (LCP) negotiated successfully], but IP could be down (IPCP negotiation failed).

The **track interface ip routing** command supports the tracking of an interface with an IP address acquired through any of the following methods:

- Conventional IP address configuration
- PPP/IPCP
- DHCP
- Unnumbered interface

---

**Examples**

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0:

```
track 1 interface serial1/0 ip routing
```

---

**Related Commands**

Command	Description
<b>show track</b>	Displays HSRP tracking information.

# track ip route

To track the state of an IP route and to enter tracking configuration mode, use the **track ip route** command in global configuration mode. To remove the tracking, use the **no** form of this command.

```
track object-number ip route ip-address/prefix-length { reachability | metric threshold }
```

```
no track object-number ip route ip-address/prefix-length { reachability | metric threshold }
```

Syntax Description		
	<i>object-number</i>	Object number that represents the object to be tracked. Range is from 1 to 500.
	<i>ip-address</i>	IP subnet address to the route that is being tracked.
	<i>/prefix-length</i>	The number of bits that comprise the address prefix. A slash must precede the value.
	<b>reachability</b>	Tracks whether the route is reachable.
	<b>metric threshold</b>	Tracks the threshold metric. The default up threshold is 254 and the default down threshold is 255.

**Defaults** The route to the subnet address is not tracked.

**Command Modes** Global 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** A tracked IP-route object is considered up and reachable when a routing-table entry exists for the route and the route is not inaccessible.

To provide a common interface to tracking clients, route metric values are normalized to the range of 0 to 255, where 0 is connected and 255 is inaccessible. The resulting value is compared against threshold values to determine the tracking state as follows:

- State is up if the scaled metric for that route is less than or equal to the up threshold.
- State is down if the scaled metric for that route is greater than or equal to the down threshold.

The tracking process uses a per-protocol configurable resolution value to convert the real metric to the scaled metric. The metric value communicated to clients is always such that a lower metric value is better than a higher metric value.

Use the **threshold metric** tracking configuration command to specify a threshold metric other than the default threshold metric.

**Examples** In the following example, the tracking process is configured to track the reachability of 10.22.0.0/16:

```
track 1 ip route 10.22.0.0/16 reachability
```

In the following example, the tracking process is configured to track the threshold metric using the default threshold metric values:

```
track 1 ip route 10.22.0.0/16 metric threshold
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show track</b>	Displays HSRP tracking information.
<b>threshold metric</b>	Sets a threshold metric other than the default value.

# track list

To specify a list of objects to be tracked and the thresholds to be used for comparison, use the **track list** command in global configuration mode. To disable the tracked list, use the **no** form of this command.

```
track object-number list {boolean {and | or}} | {threshold {weight | percentage}}
```

```
no track object-number list {boolean {and | or}} | {threshold {weight | percentage}}
```

Syntax Description	
<i>object-number</i>	Object number of the object to be tracked. Range is from 1 to 500.
<b>boolean</b>	State of the tracked list is based on a boolean calculation. The keywords are as follows: <ul style="list-style-type: none"> <li><b>and</b>—Specifies that the list is “up” if <i>all</i> objects are up, or “down” if <i>one or more</i> objects are down. For example when tracking two interfaces, “up” means that <i>both</i> interfaces are up, and “down” means that <i>either</i> interface is down.</li> <li><b>or</b>—Specifies that the list is “up” if <i>at least</i> one objects is up. For example, when tracking two interfaces, “up” means that <i>either</i> interface is up, and “down” means that <i>both</i> interfaces are down.</li> </ul>
<b>threshold</b>	State of the tracked list is based on a threshold. The keywords are as follows: <ul style="list-style-type: none"> <li><b>percentage</b>—Specifies that the threshold is based on a percentage.</li> <li><b>weight</b>—Specifies that the threshold is based on a weight.</li> </ul>

**Defaults** The list is not tracked.

**Command Modes** Global 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** A track list object may be configured to track two serial interfaces when both serial interfaces are “up” and when either serial interface is “down,” for example:

```
track 1 interface serial2/0 line-protocol
track 2 interface serial2/1 line-protocol
track 100 list boolean and
  object 1
  object 2
```

A track list object may be configured to track two serial interfaces when either serial interface is “up” and when both serial interfaces are “down,” for example:

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



```
track 101 list boolean or
  object 1
  object 2
```

A track list object may be configured to track two serial interfaces when both serial interfaces are “up” and when both serial interface is “down,” for example:

```
track 1 interface serial2/0 line-protocol
track 2 interface serial2/1 line-protocol
track 102 threshold weight
  object 1 weight 10
  object 2 weight 10
threshold weight up 20 down 0
```

The configuration shown above provides some hysteresis in case one of the serial interfaces is flapping.

#### Related Commands

Command	Description
<b>show track</b>	Displays tracking information.
<b>track object</b>	Tracks an object for a tracked list as to the up and down object states.
<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.

# track resolution

To specify resolution parameters for a tracked object, use the **track resolution** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
track resolution ip route { eigrp resolution-value | isis resolution-value | ospf resolution-value | static resolution-value }
```

```
no track resolution ip route { eigrp resolution-value | isis resolution-value | ospf resolution-value | static resolution-value }
```

<b>Syntax Description</b>	<p><b>ip route</b> IP route for metric resolution for a specified track. The keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <b>eigrp</b>—EIGRP routing protocol. The <i>resolution-value</i> argument has a range from 256 to 40000000.</li> <li>• <b>isis</b>—ISIS routing protocol. The <i>resolution-value</i> argument has a range from 1 to 1000.</li> <li>• <b>ospf</b>—OSPF routing protocol. The <i>resolution-value</i> argument has a range from 1 to 1562.</li> <li>• <b>static</b>—Static route. The <i>resolution-value</i> argument has a range from 1 to 100000.</li> </ul>
---------------------------	---

**Defaults** The track ip route metric resolution default values are used.

**Command Modes** Global configuration

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

**Usage Guidelines** The **track ip route** command causes tracking of a route in the routing table. If a route exists in the table, the metric value is converted into a number in the range from 0 to 255. The metric resolution for the specified routing protocol is used to do the conversion. There are default values for the metric resolution but the track resolution command can be used to change the metric resolution default values.

**Examples** In the following example, the EIGRP routing protocol has a resolution value of 280.

```
track resolution ip route eigrp 280
```

---

**Related Commands**

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

# track rtr

To track the state of a Service Assurance Agent (SAA) operation and to enter tracking configuration mode, use the **track rtr** command in global configuration mode. To remove the tracking, use the **no** form of this command.

```
track object-number rtr saa-id {state | reachability}
```

```
no track object-number rtr saa-id {state | reachability}
```

Syntax Description		
	<i>object-number</i>	Object number representing the object to be tracked. The range is from 1 to 500.
	<i>saa-id</i>	Service Assurance Agent router ID number.
	<b>state</b>	Tracks operation return code.
	<b>reachability</b>	Tracks whether the route is reachable.

**Defaults** SAA tracking is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.3(4)T	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

**Usage Guidelines** Every SAA operation maintains an operation return-code value. This return code is interpreted by the tracking process. The return code may return OK, OverThreshold, and several other return codes. Different operations may have different return-code values, so only values common to all operation types are used.

Two aspects of an SAA operation can be tracked: state and reachability. The difference between these relates to the acceptance of the OverThreshold return code. [Table 46](#) shows the state and reachability aspects of SAA operations that can be tracked.

**Table 46** *Comparison of State and Reachability Operations*

Tracking	Return Code	Track State
State	OK	Up
	(everything else)	Down
Reachability	OK or over threshold	Up
	(everything else)	Down

In the following example, the tracking process is configured to track the state of SAA router 2.

```
track 1 rtr 2 state
```

In the following example, the SAA tracking process is configured to track the reachability of SAA router 3.

```
track 2 rtr 3 reachability
```

# track timer

To specify the interval in which the tracking process polls the tracked object, use the **track timer** command in tracking configuration mode. To disable this functionality, use the **no** form of this command.

**track timer** {**interface** | **ip route**} *seconds*

**no track timer** {**interface** | **ip route**} *seconds*

Syntax Description		
	<b>interface</b>	Tracks the specified interface.
	<b>ip route</b>	Tracks the specified IP route.
	<i>seconds</i>	Interval (in seconds) in which the tracking process polls the object. The range is from 1 to 3000. The interface polling interval default is 1 second, and the IP-route polling interval default is 15 seconds.

**Defaults** If you do not use the **track timer** command to specify a polling interval, a tracked object will be tracked at the default polling interval.

**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.

**Examples** In the following example, the tracking process is configured to poll the tracked interface every 3 seconds:

```
track timer interface 3
```

# transmit-interface

To assign a transmit interface to a receive-only interface, use the **transmit-interface** command in interface configuration mode. To return to normal duplex Ethernet interfaces, use the **no** form of this command.

**transmit-interface** *type number*

**no transmit-interface**

Syntax Description	<i>type</i>	Transmit interface type to be linked with the (current) receive-only interface.
	<i>number</i>	Transmit interface number to be linked with the (current) receive-only interface.

**Defaults** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Usage Guidelines** Receive-only interfaces are used commonly with microwave Ethernet links.

**Examples** The following example specifies Ethernet interface 0 as a simplex Ethernet interface:

```
interface ethernet 1
 ip address 128.9.1.2
 transmit-interface ethernet 0
```

# update arp

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

**update arp**

**no update arp**

**Syntax Description** This command has no keywords or arguments.

**Defaults** No default behavior or values.

**Command Modes** DHCP pool configuration

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

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

This command can be configured only under the following conditions:

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

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



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

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

```
Router(config)# ip dhcp pool WIRELESS-POOL
Router(dhcp-config)# update arp
```



```
Router (dhcp-config) # exit
```

---

**Related Commands**

Command	Description
<b>accounting (DHCP)</b>	Enables DHCP accounting for the specified server group.
<b>aaa accounting</b>	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
<b>aaa group server</b>	Groups different server hosts into distinct lists and distinct methods.
<b>aaa new-model</b>	Enables the AAA access control model.
<b>aaa session-id</b>	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
<b>clear arp-cache</b>	Deletes all dynamic entries from the ARP cache.
<b>clear ip dhcp binding</b>	Deletes an automatic address binding from the Cisco IOS DHCP Server database.
<b>ip dhcp database</b>	Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.
<b>ip dhcp pool</b>	Configures a DHCP address pool on a Cisco IOS DHCP Server and enters DHCP pool configuration mode.
<b>ip radius source-interface</b>	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
<b>radius-server host</b>	Specifies a RADIUS server host.
<b>radius-server retransmit</b>	Specifies the number of times that Cisco IOS will look for RADIUS server hosts.
<b>show ip dhcp binding</b>	Displays address bindings on the Cisco IOS DHCP server.
<b>show ip dhcp server statistics</b>	Displays Cisco IOS DHCP server statistics.

# utilization mark high

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

**utilization mark high** *percentage-number*

**no utilization mark high** *percentage-number*

<b>Syntax Description</b>	<i>percentage-number</i> Percentage of the current pool size.
---------------------------	---

<b>Defaults</b>	The default high utilization mark is 100 percent of the current pool size.
-----------------	--

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-right: none;">Release</th> <th style="border-left: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-right: none;">12.2(8)T</td> <td style="border-left: none;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.2(8)T	This command was introduced.
Release	Modification				
12.2(8)T	This command was introduced.				

<b>Usage Guidelines</b>	<p>The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level exceeds the configured high utilization mark, the pool will schedule a subnet request.</p> <p>This command cannot be used unless the <b>autogrow size</b> option of the <b>origin</b> command is configured.</p>
-------------------------	--

<b>Examples</b>	<p>The following example sets the high utilization mark to 80 percent of the current pool size:</p> <pre>utilization mark high 80</pre>
-----------------	---

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th style="border-right: none;">Command</th> <th style="border-left: none;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-right: none;"><b>origin</b></td> <td style="border-left: none;">Configures an address pool as an on-demand address pool.</td> </tr> <tr> <td style="border-right: none;"><b>utilization mark low</b></td> <td style="border-left: none;">Configures the low utilization mark of the current address pool size.</td> </tr> </tbody> </table>	Command	Description	<b>origin</b>	Configures an address pool as an on-demand address pool.	<b>utilization mark low</b>	Configures the low utilization mark of the current address pool size.
Command	Description						
<b>origin</b>	Configures an address pool as an on-demand address pool.						
<b>utilization mark low</b>	Configures the low utilization mark of the current address pool size.						

# utilization mark low

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

**utilization mark low** *percentage-number*

**no utilization mark low** *percentage-number*

## Syntax Description

<i>percentage-number</i>	Percentage of the current pool size.
--------------------------	--------------------------------------

## Defaults

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

## Command Modes

DHCP pool configuration

## Command History

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

## Usage Guidelines

The current pool size is the sum of all addresses in all the subnets in the pool. If the utilization level drops below the configured low utilization mark, a subnet release is scheduled from the address pool. This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured.

## Examples

The following example sets the low utilization mark to 20 percent of the current pool size:

```
utilization mark low 20
```

## Related Commands

Command	Description
<b>origin</b>	Configures an address pool as an on-demand address pool.
<b>utilization mark high</b>	Configures the high utilization mark of the current address pool size.

# virtual

To configure virtual server attributes, use the **virtual** virtual server configuration command. To remove the attributes, use the **no** form of this command.

**virtual** *ip-address* {**tcp** | **udp**} *port-number* [**service** *service-name*]

**no virtual**

<b>Syntax Description</b>	<i>ip-address</i>	IP address for this virtual server instance, used by clients to connect to the server farm.
<b>tcp</b>		Performs load balancing for only TCP connections.
<b>udp</b>		Performs load balancing for only UDP connections.
<i>port-number</i>		<p>(Optional) IOS SLB virtual port (the TCP or UDP port number or port name). If specified, only the connections for the specified port on the server are load balanced. The ports and the valid name or number for the <i>port-number</i> argument are as follows:</p> <ul style="list-style-type: none"> <li>• Domain Name System: <b>dns 53</b></li> <li>• File Transfer Protocol: <b>ftp 21</b></li> <li>• HTTP over Secure Socket Layer: <b>https 443</b></li> <li>• Mapping of Airline Traffic over IP, Type A: <b>matip-a 350</b></li> <li>• Network News Transport Protocol: <b>nntp 119</b></li> <li>• Post Office Protocol v2: <b>pop2 109</b></li> <li>• Post Office Protocol v3: <b>pop3 110</b></li> <li>• Simple Mail Transport Protocol: <b>smtp 25</b></li> <li>• Telnet: <b>telnet 23</b></li> <li>• World Wide Web (HTTP): <b>www 80</b></li> </ul> <p>Specify a port number of <b>0</b> to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports).</p>
<b>service</b>		(Optional) Couple connections associated with a given service, such as HTTP or Telnet, so all related connections from the same client use the same real server.
<i>service-name</i>		(Optional) Type of connection coupling. Currently, the only choice is <b>ftp</b> . Couple FTP data connections with the control session that created them.

**Defaults** No default behavior or values.

**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.

**Usage Guidelines**

The **no virtual** command is allowed only if the virtual server was removed from service by the **no inservice** command.

For some applications, it is not feasible to configure all the virtual server TCP or UDP port numbers for the IOS SLB feature. To support such applications, you can configure IOS SLB virtual servers to accept flows destined for all ports. To configure an all-port virtual server, specify a port number of **0**.

**Note**

In general, you should use port-bound virtual servers instead of all-port virtual servers. When you use all-port virtual servers, flows can be passed to servers for which no application port exists. When servers reject these flows, IOS SLB might fail the server and remove it from load balancing.

**Examples**

The following example specifies that the virtual server with the IP address 10.0.0.1 performs load balancing for TCP connections for the port named www. The virtual server processes HTTP requests.

```
ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
```

**Related Commands**

Command	Description
<b>ip slb vserver</b>	Identifies a virtual server.
<b>show ip slb vservers</b>	Displays information about the virtual servers.

## vrf (DHCP pool)

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

**vrf** *name*

**no vrf** *name*

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

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	DHCP pool configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(8)T	This command was introduced.

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

<b>Examples</b>	The following example associates the on-demand address pool with a VRF named red:
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>origin</b>	Configures an address pool as an on-demand address pool.

# vrrp authentication

To authenticate Virtual Router Redundancy Protocol (VRRP) packets received from other routers in the group, use the **vrrp authentication** command in interface configuration mode. To disable VRRP authentication, use the **no** form of this command.

```
vrrp group authentication {text string | md5 key-string [0 | 7] key | key-chain key-chain} [timeout seconds]
```

```
no vrrp group authentication string {md5 key-string [0 | 7] key | key-chain key-chain} [timeout seconds]
```

Syntax Description	
<i>group</i>	Virtual router group number for which authentication is being configured. The group number is configured with the <b>vrrp ip</b> command.
<b>text</b>	Text for authentication. The <i>string</i> argument can have up to eight alphanumeric characters and is used to validate incoming VRRP packets.
<b>md5</b>	<p>Message Digest 5 (MD5) authentication. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>key-string</b>—Authentication using up to 64 characters. It is recommended that at least 16 characters be used. The arguments and keywords are as follows: <ul style="list-style-type: none"> <li>– <b>0</b>—(Optional) No prefix to the key argument or specifying 0 means the key will be unencrypted.</li> <li>– <b>7</b>—(Optional) The key will be encrypted.</li> <li>– <i>key</i>—Up to 64 characters in length. It is recommended that at least 16 characters be used.</li> </ul> </li> <li>• <b>key-chain</b>—Authentication using a live key and key ID. The <i>key-chain</i> argument specifies the key chain. The <i>key-chain</i> argument must match the assigned key-chain name using the <b>key chain</b> command.</li> </ul> <p><b>Note</b> The key-string authentication method is encrypted if the <b>service password encryption</b> command has been specified.</p>
<i>timeout</i>	<p>(Optional) Time period, in seconds, that the VRRP group will accept MD5 digests based on the old and new keys. The <i>seconds</i> argument ?</p> <p><i>The seconds argument has a range from 1 to 60? The default is ?</i></p>

**Defaults** No authentication of VRRP messages occurs.

**Command Modes** Interface configuration

**Command History**

Release	Modification
12.0(18)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(106)T	The <b>text</b> , <b>md5</b> , <b>key-string</b> , <b>0</b> , <b>7</b> , <b>timeout</b> , and <b>key-chain</b> keywords were added. The <i>key</i> , <i>seconds</i> , and <i>key-chain arguments</i> were added.

**Usage Guidelines**

When a VRRP packet arrives from another router in the VRRP group, its authentication string is compared to the string configured on the local system. If the strings match, the message is accepted. If they do not match, the packet is discarded.

All routers within the group must be configured with the same authentication string.

Note that plain text authentication is not meant to be used for security. It simply provides a way to prevent a misconfigured router from participating in VRRP.

**Examples**

The following example shows how to configure an authentication string of x30dn78k:

```
vrrp 1 authentication x30dn78k
```

The following example shows how to configure an MD5 key string and a timeout of 30 seconds:

```
interface Ethernet0/1
  description ed1-cat5a-7/10
  vrrp 1 ip 10.21.0.10
  vrrp 1 priority 110
  vrrp 1 authentication md5 key-string f00c4s timeout 30
```

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

**Router 1**

```
key chain vrrp1
  key 0
  key-string 54321098452103ab
!
interface Ethernet0/1
  vrrp 1 ip 10.21.0.10
  vrrp 1 authentication md5 key-chain vrrp1
```

**Router 2**

```
interface Ethernet0/1
  vrrp 1 ip 10.21.0.10
  vrrp 1 authentication md5 key-string 54321098452103ab
```

**Related Commands**

Command	Description
<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.



# vrrp description

To assign a description to the Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp description** command in interface configuration mode. To remove the description, use the **no** form of this command.

```
vrrp group description text
```

```
no vrrp group description
```

## Syntax Description

<i>group</i>	Virtual router group number.
<i>text</i>	Text (up to 80 characters) that describes the purpose or use of the group.

## Defaults

There is no description of the VRRP group.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Examples

The following example enables VRRP on Ethernet interface 0. VRRP group 1 is described as Building A — Marketing and Administration.

```
interface ethernet 0
 ip address 10.0.1.1 255.255.255.0
!
 vrrp 1 ip 10.0.1.20
 vrrp 1 description Building A - Marketing and Administration
```

## Related Commands

Command	Description
<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.

# vrrp ip

To enable the Virtual Router Redundancy Protocol (VRRP) on an interface and identify the IP address of the virtual router, use the **vrrp ip** command in interface configuration mode. To disable VRRP on the interface and remove the IP address of the virtual router, use the **no** form of this command.

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

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

## Syntax Description

<i>group</i>	Virtual router group number.
<i>ip-address</i>	IP address of the virtual router.
<b>secondary</b>	(Optional) Indicates additional IP addresses supported by this group.

## Defaults

VRRP is not configured on the interface.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

## Usage Guidelines

Configure this command once without the **secondary** keyword to indicate the virtual router IP address. If you want to indicate additional IP addresses supported by this group, then do so and include the **secondary** keyword.

Note that removing the VRRP configuration from the IP address owner and leaving the IP address of the interface active is considered a misconfiguration because duplicate IP addresses on the LAN will result.

## Examples

The following example enables VRRP on Ethernet interface 0. The VRRP group is 1. IP address 10.0.1.20 is the address of the virtual router.

```
interface ethernet 0
 ip address 10.0.1.1 255.255.255.0
 ip address 10.0.2.1 255.255.255.0 secondary
!
vrrp 1 ip 10.0.1.20
vrrp 1 ip 10.0.2.20 secondary
```

Related Commands	Command	Description
	<b>show vrrp</b>	Displays a summary or detailed status of one or all configured VRRP groups.

## vrrp preempt

To configure the router to take over as master virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current master virtual router, use the **vrrp preempt** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**vrrp group preempt [delay seconds]**

**no vrrp group preempt**

<b>Syntax Description</b>	<i>group</i>	Virtual router group number of the group for which preemption is being configured. The group number is configured with the <b>vrrp ip</b> command.
	<b>delay seconds</b>	(Optional) Number of seconds that the router will delay before issuing an advertisement claiming master ownership. The default delay is 0 seconds.

**Defaults** Enabled

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
		12.0(18)ST
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** By default, the router being configured with this command will take over as master virtual router for the group if it has a higher priority than the current master virtual router. You can configure a delay, which will cause the VRRP router to wait the specified number of seconds before issuing an advertisement claiming master ownership.

Note that the router that is the IP address owner will preempt, regardless of the setting of this command.

**Examples** The following example configures the router to preempt the current master virtual router when its priority of 200 is higher than that of the current master virtual router. If the router preempts the current master virtual router, it waits 15 seconds before issuing an advertisement claiming it is the master virtual router.

```
vrrp 1 preempt delay 15
vrrp 1 priority 200
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.
<b>vrrp priority</b>	Sets the priority level of the router within a VRRP group.

## vrrp priority

To set the priority level of the router within a Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp priority** command in interface configuration mode. To remove the priority level of the router, use the **no** form of this command.

**vrrp** *group* **priority** *level*

**no vrrp** *group* **priority** *level*

Syntax Description	group	Virtual router group number.
	level	Priority of the router within the VRRP group. The range is from 1 to 254. The default is 100.

**Defaults** *level*: 100

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(18)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** Use this command to control which router becomes the master virtual router.

**Examples** The following example configures the router with a priority of 254:

```
vrrp 1 priority 254
```

Related Commands	Command	Description
	<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.
	<b>vrrp preempt</b>	Configures the router to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual router.

# vrrp timers advertise

To configure the interval between successive advertisements by the master virtual router in a Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp timers advertise** command in interface configuration mode. To restore the default value, use the **no** form of this command.

```
vrrp group timers advertise [msec] interval
```

```
no vrrp group timers advertise [msec] interval
```

Syntax Description		
	<i>group</i>	Virtual router group number.
	<b>msec</b>	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.
	<i>interval</i>	Time interval between successive advertisements by the master virtual router. The unit of the interval is in seconds, unless the <b>msec</b> keyword is specified. The default is 1 second.

**Defaults** *interval*: 1 second

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(18)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

**Usage Guidelines** The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

**Examples** The following example configures the master virtual router to send advertisements every 4 seconds:

```
vrrp 1 timers advertise 4
```

Related Commands	Command	Description
	<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.
	<b>vrrp timers learn</b>	Configures the router, when it is acting as backup virtual router for a VRRP group, to learn the advertisement interval used by the master virtual router.

# vrrp timers learn

To configure the router, when it is acting as backup virtual router for a Virtual Router Redundancy Protocol (VRRP) group, to learn the advertisement interval used by the master virtual router, use the **vrrp timers learn** command in interface configuration mode. To prevent the local router from learning the advertisement interval of the master virtual router, use the **no** form of this command.

**vrrp group timers learn**

**no vrrp group timers learn**

<b>Syntax Description</b>	<i>group</i>	Virtual router group number to which the command applies.
<b>Defaults</b>	Disabled; the local router calculates the downtime of the master virtual router based on the advertisement interval of the local router as configured by the <b>vrrp timers advertise</b> command.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(18)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
<b>Usage Guidelines</b>	If this command is configured, when the local router is acting as a backup virtual router for the group, it will learn the advertisement interval of the current master virtual router from its master advertisements. The local router will use that value to calculate how long it should wait before deciding that the master virtual router has gone down. This command synchronizes timers with the current master virtual router.	
<b>Examples</b>	The following example configures the router, when it is acting as backup virtual router, to learn the advertisement interval from the advertisements of the current master virtual router:  vrrp 1 timers learn	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.
	<b>vrrp timers advertise</b>	Configures the interval between successive advertisements by the master virtual router in a VRRP group.



# vrrp track

To configure the Virtual Router Redundancy Protocol (VRRP) to track an object, use the **vrrp track** command in interface configuration mode. To disable the tracking, use the **no** form of this command.

```
vrrp [group-number] track object-number [decrement priority]
```

```
no vrrp [group-number] track object-number [decrement priority]
```

Syntax Description	
<i>group-number</i>	(Optional) Group number to which the tracking applies.
<i>object-number</i>	Object number in the range from 1 to 500 representing the object to be tracked.
<b>decrement</b> <i>priority</i>	(Optional) Amount by which the priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). The default value is 10. Decrements can be set to any value between 1 and 255.

**Defaults** The default decrement value is 10. The range is from 1 and 255.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.3(2)T	This command was introduced.

**Usage Guidelines** You can configure VRRP to track specific objects, such as an interface or IP route, that can alter the priority level of a virtual router for a VRRP group. The tracked objects are first defined using the **track interface** or **track ip route** global configuration command. The client process, in this case VRRP, registers interest in tracking these objects and can then be notified when the tracked object changes state.

**Examples** In the following example, the tracking process is configured to track the IP routing capability of serial interface 1/0. VRRP on Ethernet interface 0/0 then registers with the tracking process to be informed of any changes to the IP routing state of serial interface 1/0. If the IP state on serial interface 1/0 goes down, then the priority of the VRRP group is reduced by 10.

If both serial interfaces are operational, then Router A will be the master virtual router because it has the higher priority.

However, if IP routing on serial interface 1/0 in Router A fails, then the HSRP group priority will be reduced and Router B will take over as the master virtual router, thus maintaining a default virtual gateway service to hosts on the 10.1.0.0 subnet.

### Router A Configuration

```
!
track 100 interface serial1/0 ip routing
!
```

```
interface Ethernet0/0
 ip address 10.1.0.21 255.255.0.0
 vrrp 1 ip 10.1.0.1
 vrrp 1 priority 105
 vrrp 1 track 100 decrement 10
```

### Router B Configuration

```
!
track 100 interface serial1/0 ip routing
!
interface Ethernet0/0
 ip address 10.1.0.22 255.255.0.0
 vrrp 1 ip 10.1.0.1
 vrrp 1 priority 100
 vrrp 1 track 100 decrement 10
```

### Related Commands

Command	Description
<b>track interface</b>	Configures an interface to be tracked.
<b>track ip route</b>	Tracks the state of an IP route.

# vrrp shutdown

To disable the Virtual Router Redundancy Protocol (VRRP) group on an interface, use the **vrrp shutdown** command in interface configuration mode.

## **vrrp group shutdown**

<b>Syntax Description</b>	<i>group</i>	Virtual router group number.
<b>Defaults</b>	Enabled	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(11)T	This command was introduced.
<b>Usage Guidelines</b>	When a VRRP group has been configured using the <b>vrrp group ip</b> command, the protocol is fully operational. The <b>vrrp shutdown</b> command is not displayed on the router, and to disable the protocol for one group, you must explicitly specify the group using the <b>vrrp shutdown</b> command.	
<b>Examples</b>	<p>The following example shows how to enable VRRP on Ethernet interface 0/2 (group 1) and disables it on Ethernet interface 0/1, group 1.</p> <pre>interface ethernet0/1  ip address 10.0.1.1 255.255.255.0  vrrp 1 ip 10.0.1.254  vrrp 1 shutdown ! interface ethernet0/2  ip address 10.0.42.1 255.255.255.0  vrrp 2 ip 10.0.42.254</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show vrrp</b>	Displays a summary or detailed status of one or all configured VRRP groups.

# weight

To specify the capacity of a real server relative to other real servers in the server farm, use the **weight** real server configuration command. To restore the default weight value, use the **no** form of this command.

**weight** *weighting-value*

**no weight**

<b>Syntax Description</b>	<i>weighting-value</i>	Weighting value to use for real server predictor algorithm. Valid values range from 1 to 155. The default weighting value is 8.
---------------------------	------------------------	---

<b>Defaults</b>	The default weighting value is 8.
-----------------	-----------------------------------

<b>Command Modes</b>	SLB real server configuration
----------------------	-------------------------------

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

**Examples** The following example specifies the relative weighting values of three real servers as 16, 8 (by default), and 24, respectively:

```
ip slb serverfarm PUBLIC
real 10.10.1.1First real server
weight 16Assigned weight of 16
inserviceEnabled
exit
real 10.10.1.2Second real server
inserviceEnabled; default weight
exit
real 10.10.1.3Third real server
weight 24Assigned weight of 24;
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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.	