

Cisco IOS IP Application Services Command Reference

November 2010

Americas 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: 408 527-0883

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS IP Application Services Command Reference
© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Introduction IAP-1

IP Application Services Commands IAP-3

- aaa accounting vrrs IAP-4
- access (firewall farm) IAP-6
- access (server farm) IAP-8
- access (virtual server) IAP-10
- accounting delay (VRRS) IAP-12
- accounting method (VRRS) IAP-14
- address (custom UDP probe) IAP-16
- address (DNS probe) IAP-17
- address (HTTP probe) IAP-18
- address (ping probe) IAP-19
- address (TCP probe) IAP-20
- address (WSP probe) IAP-21
- advertise IAP-23
- agent IAP-25
- apn IAP-27
- attribute list (VRRS) IAP-28
- bindid IAP-30
- calling-station-id IAP-32
- carrier-delay (tracking) IAP-33
- clear fm slb counters IAP-35
- clear ip accounting IAP-36
- clear ip icmp rate-limit IAP-37
- clear ip sctp statistics IAP-38
- clear ip slb connections IAP-40
- clear ip slb counters IAP-42
- clear ip slb sessions IAP-43
- clear ip slb sticky asn msid IAP-44
- clear ip slb sticky gtp imsi IAP-45

clear ip slb sticky radius **IAP-46**
clear ip tcp header-compression **IAP-48**
clear ip traffic **IAP-49**
clear ip wccp **IAP-50**
clear mls acl counters **IAP-52**
clear platform software wccp **IAP-54**
clear sctp statistics **IAP-55**
clear sockets **IAP-57**
clear tcp statistics **IAP-58**
clear time-range ipc **IAP-59**
client (virtual server) **IAP-60**
credentials (HTTP probe) **IAP-62**
default (tracking) **IAP-63**
default-state **IAP-65**
delay (firewall farm TCP protocol) **IAP-66**
delay (tracking) **IAP-67**
delay (virtual server) **IAP-68**
expect **IAP-70**
failaction (firewall farm) **IAP-72**
failaction (server farm) **IAP-73**
faildetect (custom UDP probe) **IAP-75**
faildetect (DNS probe) **IAP-76**
faildetect (ping probe) **IAP-77**
faildetect inband (real server) **IAP-78**
faildetect numconns (real server) **IAP-80**
farm-weight **IAP-82**
forwarding-agent **IAP-83**
glbp authentication **IAP-84**
glbp client-cache maximum **IAP-86**
glbp forwarder preempt **IAP-88**
glbp ip **IAP-89**
glbp load-balancing **IAP-91**
glbp name **IAP-93**
glbp preempt **IAP-95**
glbp priority **IAP-96**

glbp sso **IAP-97**
glbp timers **IAP-98**
glbp timers redirect **IAP-100**
glbp weighting **IAP-102**
glbp weighting track **IAP-104**
gtp notification cac **IAP-106**
gtp session (virtual server) **IAP-107**
gw port (virtual server) **IAP-108**
hand-off radius **IAP-109**
header **IAP-110**
idle (firewall farm datagram protocol) **IAP-112**
idle (firewall farm TCP protocol) **IAP-113**
idle (virtual server) **IAP-115**
inservice (DFP agent) **IAP-118**
inservice (firewall farm) **IAP-120**
inservice (firewall farm real server) **IAP-121**
inservice (server farm real server) **IAP-122**
inservice (server farm virtual server) **IAP-123**
interval (custom UDP probe) **IAP-125**
interval (DFP agent) **IAP-126**
interval (DNS probe) **IAP-127**
interval (HTTP probe) **IAP-128**
interval (ping probe) **IAP-129**
interval (TCP probe) **IAP-130**
interval (WSP probe) **IAP-131**
ip accounting **IAP-132**
ip accounting-list **IAP-134**
ip accounting mac-address **IAP-136**
ip accounting precedence **IAP-138**
ip accounting-threshold **IAP-139**
ip accounting-transits **IAP-141**
ip broadcast-address **IAP-142**
ip casa **IAP-143**
ip cef traffic-statistics **IAP-145**
ip dfp agent **IAP-147**

ip directed-broadcast **IAP-148**
ip forward-protocol **IAP-150**
ip forward-protocol spanning-tree **IAP-152**
ip forward-protocol turbo-flood **IAP-154**
ip header-compression special-vj **IAP-156**
ip helper-address **IAP-158**
ip icmp rate-limit unreachable **IAP-160**
ip icmp redirect **IAP-162**
ip information-reply **IAP-164**
ip irdp **IAP-165**
ip mask-reply **IAP-167**
ip mtu **IAP-168**
ip redirects **IAP-170**
ip sctp asconf **IAP-171**
ip sctp authenticate **IAP-173**
ip slb capp udp **IAP-175**
ip slb dfp **IAP-176**
ip slb entries **IAP-178**
ip slb firewallfarm **IAP-183**
ip slb map **IAP-184**
ip slb maxbuffers frag **IAP-186**
ip slb natpool **IAP-187**
ip slb probe custom udp **IAP-189**
ip slb probe dns **IAP-191**
ip slb probe http **IAP-192**
ip slb probe ping **IAP-194**
ip slb probe tcp **IAP-195**
ip slb probe wsp **IAP-196**
ip slb replicate slave rate **IAP-197**
ip slb route **IAP-199**
ip slb serverfarm **IAP-201**
ip slb static **IAP-202**
ip slb timers gtp gsn **IAP-204**
ip slb vserver **IAP-205**
ip tcp adjust-mss **IAP-206**

ip tcp chunk-size **IAP-208**
ip tcp compression-connections **IAP-209**
ip tcp ecn **IAP-211**
ip tcp header-compression **IAP-212**
ip tcp mss **IAP-215**
ip tcp path-mtu-discovery **IAP-217**
ip tcp queuemax **IAP-218**
ip tcp selective-ack **IAP-219**
ip tcp synwait-time **IAP-221**
ip tcp timestamp **IAP-222**
ip tcp window-size **IAP-223**
ip unreachables **IAP-225**
ip vrf **IAP-226**
ip vrf (tracking) **IAP-228**
ip wccp **IAP-230**
ip wccp check acl outbound **IAP-235**
ip wccp check services all **IAP-236**
ip wccp enable **IAP-238**
ip wccp group-listen **IAP-239**
ip wccp outbound-acl-check **IAP-241**
ip wccp redirect **IAP-242**
ip wccp redirect exclude in **IAP-245**
ip wccp redirect-list **IAP-246**
ip wccp source-interface **IAP-247**
ip wccp version **IAP-249**
ip wccp web-cache accelerated **IAP-250**
kal-ap domain **IAP-252**
lookup **IAP-253**
manager (DFP agent) **IAP-254**
maxclients **IAP-255**
maxconns (firewall farm datagram protocol) **IAP-257**
maxconns (firewall farm TCP protocol) **IAP-258**
maxconns (server farm) **IAP-259**
mls aging slb normal **IAP-260**
mls aging slb process **IAP-261**

mls ip install-threshold **IAP-262**
mls ip reflexive ndr-entry tcam **IAP-263**
mls ip slb purge global **IAP-264**
mls ip slb search wildcard **IAP-265**
nat **IAP-267**
object (tracking) **IAP-269**
password (DFP agent) **IAP-271**
peer port **IAP-273**
peer secret **IAP-274**
platform trace runtime process forwarding-manager module wccp **IAP-276**
port (custom UDP probe) **IAP-278**
port (DFP agent) **IAP-279**
port (HTTP probe) **IAP-280**
port (TCP probe) **IAP-281**
predictor **IAP-282**
predictor hash address (firewall farm) **IAP-284**
probe (firewall farm real server) **IAP-285**
probe (server farm) **IAP-286**
protocol datagram **IAP-287**
protocol tcp **IAP-288**
purge connection **IAP-289**
purge radius framed-ip acct on-off **IAP-290**
purge radius framed-ip acct stop **IAP-291**
purge sticky **IAP-292**
radius acct local-ack key **IAP-293**
radius inject acct key **IAP-295**
radius inject auth **IAP-297**
radius inject auth timer **IAP-299**
radius inject auth vsa **IAP-300**
rate **IAP-301**
real (firewall farm) **IAP-303**
real (server farm) **IAP-304**
real (static NAT) **IAP-306**
reassign **IAP-307**
replicate casa (firewall farm) **IAP-309**

replicate casa (virtual server) **IAP-311**
replicate interval (firewall farm) **IAP-314**
replicate interval (virtual server) **IAP-316**
replicate slave (firewall farm) **IAP-318**
replicate slave (virtual server) **IAP-320**
request (custom UDP probe) **IAP-322**
request (HTTP probe) **IAP-324**
response **IAP-326**
retry (real server) **IAP-327**
sctp **IAP-329**
serverfarm **IAP-331**
service-module ip redundancy **IAP-334**
show debugging **IAP-336**
show fm slb counters **IAP-339**
show glbp **IAP-340**
show interface mac **IAP-347**
show interface precedence **IAP-349**
show ip accounting **IAP-351**
show ip casa affinities **IAP-354**
show ip casa oper **IAP-356**
show ip casa stats **IAP-358**
show ip casa wildcard **IAP-360**
show ip dfp **IAP-363**
show ip helper-address **IAP-366**
show ip icmp rate-limit **IAP-368**
show ip redirects **IAP-370**
show ip sctp association list **IAP-371**
show ip sctp association parameters **IAP-373**
show ip sctp association statistics **IAP-377**
show ip sctp errors **IAP-379**
show ip sctp instances **IAP-381**
show ip sctp statistics **IAP-383**
show ip slb conns **IAP-385**
show ip slb dfp **IAP-387**
show ip slb firewallfarm **IAP-390**

show ip slb fragments **IAP-392**
show ip slb gtp **IAP-393**
show ip slb map **IAP-396**
show ip slb natpool **IAP-398**
show ip slb probe **IAP-400**
show ip slb reals **IAP-402**
show ip slb replicate **IAP-407**
show ip slb serverfarms **IAP-409**
show ip slb sessions **IAP-411**
show ip slb static **IAP-415**
show ip slb stats **IAP-417**
show ip slb sticky **IAP-421**
show ip slb vservers **IAP-426**
show ip slb wildcard **IAP-433**
show ip sockets **IAP-434**
show ip tcp header-compression **IAP-436**
show ip traffic **IAP-439**
show ip wccp **IAP-443**
show ip wccp global counters **IAP-454**
show ip wccp web-caches **IAP-455**
show platform hardware qfp active feature wccp **IAP-456**
show platform software wccp **IAP-458**
show sctp association **IAP-462**
show sctp association list **IAP-464**
show sctp association parameters **IAP-466**
show sctp association statistics **IAP-470**
show sctp errors **IAP-472**
show sctp instance **IAP-474**
show sctp instances **IAP-476**
show sctp statistics **IAP-478**
show sockets **IAP-480**
show standby **IAP-484**
show standby arp gratuitous **IAP-490**
show standby capability **IAP-491**
show standby delay **IAP-493**

show standby internal **IAP-494**
show standby neighbors **IAP-497**
show standby redirect **IAP-499**
show tcp **IAP-502**
show tcp brief **IAP-511**
show tcp statistics **IAP-513**
show tech-support **IAP-518**
show time-range ipc **IAP-525**
show track **IAP-526**
show udp **IAP-531**
show vrrp **IAP-533**
show vrrp interface **IAP-537**
show vrrs clients **IAP-539**
show vrrs group **IAP-541**
show vrrs plugin database **IAP-543**
show vrrs summary **IAP-545**
snmp-server enable traps slb **IAP-547**
special-vj **IAP-548**
standby arp gratuitous **IAP-549**
standby authentication **IAP-551**
standby bfd **IAP-553**
standby bfd all-interfaces **IAP-554**
standby delay minimum reload **IAP-556**
standby follow **IAP-558**
standby ip **IAP-560**
standby mac-address **IAP-562**
standby mac-refresh **IAP-564**
standby name **IAP-565**
standby preempt **IAP-566**
standby priority **IAP-569**
standby redirect **IAP-571**
standby redirects (global) **IAP-573**
standby send arp **IAP-574**
standby sso **IAP-575**
standby timers **IAP-576**

standby track **IAP-578**
standby use-bia **IAP-582**
standby version **IAP-584**
start-forwarding-agent **IAP-586**
sticky (firewall farm datagram protocol) **IAP-587**
sticky (firewall farm TCP protocol) **IAP-588**
sticky (virtual server) **IAP-589**
synguard (virtual server) **IAP-592**
threshold metric **IAP-594**
threshold percentage **IAP-596**
threshold weight **IAP-598**
timeout (custom UDP probe) **IAP-600**
track **IAP-601**
track application **IAP-603**
track interface **IAP-605**
track ip route **IAP-607**
track ip sla **IAP-609**
track list **IAP-611**
track resolution **IAP-613**
track rtr **IAP-615**
track stub-object **IAP-617**
track timer **IAP-619**
url (WSP probe) **IAP-621**
username (IOS SLB) **IAP-622**
virtual **IAP-624**
vrrp authentication **IAP-628**
vrrp delay **IAP-631**
vrrp description **IAP-633**
vrrp ip **IAP-634**
vrrp name **IAP-636**
vrrp preempt **IAP-637**
vrrp priority **IAP-639**
vrrp shutdown **IAP-641**
vrrp sso **IAP-643**
vrrp timers advertise **IAP-644**

vrrp timers learn **IAP-646**
vrrp track **IAP-648**
vrrs **IAP-650**
vrrs follow **IAP-652**
vrrs interface-state **IAP-653**
vrrs mac-address **IAP-655**
weight (firewall farm real server) **IAP-657**
weight (real server) **IAP-658**



Introduction

This document describes the commands used to configure and monitor the following IP application services capabilities and features:

- Enhanced OBject Tracking (EOT)
- First Hop Redundancy Protocols (FHRP)
- ICMP Router Discovery Protocol (IRDP)
- IP Services
- IPv4 Broadcast Packet Handling
- Server Load Balancing (SLB)
- Stream Control Transmission Protocol (SCTP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Web Cache Control Protocol (WCCP)

For IP application services configuration tasks and examples, refer to the *Cisco IOS IP Application Services Configuration Guide*.



IP Application Services Commands

aaa accounting vrrs

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use the Virtual Router Redundancy Service (VRRS), use the **aaa accounting vrrs** command in global configuration mode. To disable AAA accounting for VRRS, use the **no** form of this command.

aaa accounting vrrs {**default** | *list-name*} **start-stop** *method1* [*method2...*]

no aaa accounting vrrs {**default** | *list-name*} **start-stop** *method1* [*method2...*]

Syntax Description

default	Uses the listed accounting methods that follow this keyword as the default list of methods for accounting services.
list-name	Character string used to name the list of accounting methods. If no list name is specified, the system uses the default value.
start-stop	Sends an accounting-on notice. The accounting-on record is sent in the background. The requested user process begins regardless of whether the accounting-on notice is received by the accounting server.
method1 [*method2...*]	(Optional) Character string used to name at least one of the accounting methods, tried in the specified sequence.

Command Default

AAA accounting is disabled for VRRS

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **aaa accounting vrrs** command to define a AAA accounting method list. If you define the AAA default accounting method list, you are defining the AAA accounting method list for all the VRRS servers. The default AAA accounting method list is applied to all VRRS groups. To specify a group-specific VRRS method list, use the **accounting method** command in VRRS configuration mode.

Examples

The following example shows how to configure VRRP group 1 with the group name “vrrp-name-1” to use VRRS method list vrrs-mlist-1:

```
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
!
Router(config-if)# vrrs vrrp-name-1
Router(config)# accounting mlist vrrs-mlist-1
!
Router(config)# interface gigabitethernet0/2/2
```

```
Router(config-if)# ip address 10.0.1.
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 1 name vrrp-name-1
```

Related Commands

Command	Description
vrrp ip	Enables the VRRP on an interface and identifies the IP address of the virtual router.
vrrp name	Links a VRRS client to a VRRP group.

access (firewall farm)

To route specific flows to a firewall farm, use the **access** command in firewall farm configuration mode. To restore the default settings, use the **no** form of this command.

access [**source** *source-ip netmask* | **destination** *destination-ip netmask* |
inbound {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]

no access [**source** *source-ip netmask* | **destination** *destination-ip netmask* |
inbound {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]

Syntax Description

source	(Optional) Routes flows based on source IP address.
source-ip	(Optional) Source IP address. The default is 0.0.0.0 (all sources).
netmask	(Optional) Source IP network mask. The default is 0.0.0.0 (all source subnets).
destination	(Optional) Routes flows based on destination IP address.
destination-ip	(Optional) Destination IP address. The default is 0.0.0.0 (all destinations).
netmask	(Optional) Destination IP network mask. The default is 0.0.0.0 (all destination subnets).
inbound *inbound-interface*	(Optional) Indicates that the firewall farm is to accept inbound packets only on the specified inbound interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *inbound-interface* argument.
inbound datagram connection	(Optional) Indicates that IOS SLB is to create connections for inbound traffic as well as outbound traffic.
outbound *outbound-interface*	(Optional) Indicates that the firewall farm is to accept outbound packets only on the specified outbound interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *outbound-interface* argument.

Defaults

The default source IP address is 0.0.0.0 (routes flows from all sources to this firewall farm).
The default source IP network mask is 0.0.0.0 (routes flows from all source subnets to this firewall farm).
The default destination IP address is 0.0.0.0 (routes flows from all destinations to this firewall farm).
The default destination IP network mask is 0.0.0.0 (routes flows from all destination subnets to this firewall farm).
If you do not specify an inbound interface, the firewall farm accepts inbound packets on all inbound interfaces.
If you do not specify the **inbound datagram connection** option, IOS SLB creates connections only for outbound traffic.
If you do not specify an outbound interface, the firewall farm accepts outbound packets on all outbound interfaces.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(7)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The **inbound** and **outbound** keywords and *inbound-interface* and *outbound-interface* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **datagram connection** keywords were added. The *inbound-interface* and *outbound-interface* arguments can be subinterfaces.

Usage Guidelines

You can specify more than one source or destination for each firewall farm. To do so, configure multiple **access** statements, making sure the network masks do not overlap each other.

You can specify up to two inbound interfaces and two outbound interfaces for each firewall farm. To do so, configure multiple **access** statements, keeping the following considerations in mind:

- All inbound and outbound interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).
- All inbound and outbound interfaces must be different from each other.
- You cannot change inbound or outbound interfaces for a firewall farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the firewall farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

By default, IOS SLB firewall load balancing creates connections only for outbound traffic (that is, traffic that arrives through the real server). Inbound traffic uses those same connections to forward the traffic, which can impact the CPU. To enable IOS SLB to create connections for both inbound traffic and outbound traffic, reducing the impact on the CPU, use the **access inbound datagram connection** command.

Examples

The following example routes flows with a destination IP address of 10.1.6.0 to firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

access (server farm)

To configure an access interface for a server farm, use the **access** command in server farm configuration mode. To disable the access interface, use the **no** form of this command.

access *interface*

no access *interface*

Syntax Description

interface	Interface to be inspected. The server farm will handle outbound flows from real servers only on the specified interface. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *interface* argument.

Defaults

The server farm handles outbound flows from real servers on all interfaces.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The *interface* argument can be a subinterface.

Usage Guidelines

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two access interfaces for each server farm. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- The access interfaces of primary and backup server farms must be the same.
- You cannot change the interfaces for a server farm while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the server farm in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

Examples

The following example limits the server farm to handling outbound flows from real servers only on access interface Vlan106:

```
Router(config)# ip slb serverfarm SF1
```

```
Router(config-slb-sfarm)# access Vlan106
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farms.

access (virtual server)

To enable framed-IP routing to inspect the ingress interface, use the **access** command in virtual server configuration mode. To disable framed-IP routing, use the **no** form of this command.

access *interface* [**route framed-ip**]

no access *interface* [**route framed-ip**]

Syntax Description

interface	Interface to be inspected. You can specify a subinterface, such as Gigabitethernet7/3.100, for the *interface* argument.
route framed-ip	(Optional) Routes flows using framed-IP routing.

Defaults

Framed-IP routing cannot inspect the ingress interface.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(12c)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The command was modified to accept up to two framed-IP access interfaces (specified on separate commands).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The *interface* argument can be a subinterface.

Usage Guidelines

This command enables framed-IP routing to inspect the ingress interface when routing subscriber traffic. All framed-IP sticky database entries created as a result of RADIUS requests to this virtual server will include the interface in the entry. In addition to matching the source IP address of the traffic with the framed-IP address, the ingress interface must also match this interface when this command is configured.

You can use this command to allow subscriber data packets to be routed to multiple service gateway service farms.

The virtual server and its associated server farm interfaces must be in the same Virtual Private Network (VPN) routing and forwarding (VRF).

You can specify up to two framed-IP access interfaces for each virtual server. To do so, configure two **access** statements, keeping the following considerations in mind:

- The two interfaces must be in the same VRF.
- The two interfaces must be different from each other.
- You cannot change the interfaces for a virtual server while it is in service.

If you do not configure an access interface using this command, IOS SLB installs the wildcards for the virtual server in all of the available interfaces of the device, including the VRF interfaces. If IOS SLB is not required on the VRF interfaces, use this command to limit wildcards to the specified interfaces only.

Examples

The following example enables framed-IP routing to inspect ingress interface Vlan20:

```
Router(config)# ip slb vserver SSG_AUTH
Router(config-slb-vserver)# access Vlan20 route framed-ip
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

accounting delay (VRRS)

To specify a delay time for sending accounting-off messages for the Virtual Router Redundancy Service (VRRS), use the **accounting delay** command in VRRS configuration mode. To return to the default accounting delay value, use the **no** form of this command.

accounting delay *seconds*

no accounting delay

Syntax Description

seconds	Time, in seconds, to wait before sending accounting-off messages. Range is from 1 to 30. The default is 0.

Command Default

Accounting-off messages for VRRS are sent without delay.

Command Modes

VRRS configuration (config-vrrs)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **accounting delay** command to control the timing of sending accounting-off messages for VRRS. This command does not apply to accounting-on messages. If the default is specified, this command is not saved to the running configuration and accounting-off messages are sent immediately when the event occurs. Otherwise, a delay of the configured number of seconds is applied.

Examples

The following example shows how to specify a delay time of 10 seconds for sending accounting-off messages for the VRRS:

```
Router(config)# vrrs vrrp-name-1
Router(config-vrrs)# accounting delay 10
```

Related Commands

Command	Description
aaa accounting vrrs	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
accounting method (VRRS)	Enables VRRS accounting for a VRRP group.
attribute list (VRRS)	Specifies additional attributes to include in VRRS accounting-on and accounting-off messages.
vrrs	Enables VRRS and enters VRRS configuration mode.

accounting method (VRRS)

To enable Virtual Router Redundancy Service (VRRS) accounting for a Virtual Router Redundancy Protocol (VRRP) group, use the **accounting method** command in VRRS configuration mode. To specify the default VRRS accounting method list as the target for VRRS accounting, use the **no** form of this command.

accounting method {**default** | *accounting-method-list*}

no accounting method

Syntax Description

default	Enables VRRS accounting for all VRRP groups.
accounting-method-list	Name of the accounting method list for which VRRS must be enabled.

Command Default

The default VRRS accounting method list is used.

Command Modes

VRRS Configuration (config-vrrs)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Configuring the **default** keyword does not save it to the running configuration and the VRRS accounting type default method list is automatically applied to the VRRS group being configured. The **default** keyword also enables VRRS accounting for all VRRP groups.

The valued specified for the *accounting-method-list* argument must match a named list configured by the **aaa accounting vrrs** command. When there is no match, a warning message is displayed. However, the configuration is still saved.

With this approach, you can configure the desired accounting method list using the **aaa accounting vrrs** command without configuring the **accounting method** command again.

Examples

The following example shows how to configure VRRS to use the accounting list named METHOD1:

```
Router(config)# vrrs VRRS1
Router(config-vrrs)# accounting method METHOD1
```

Related Commands

Command	Description
aaa accounting vrrs	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
accounting delay (VRRS)	Specifies a delay time for sending accounting-off messages for VRRS.
attribute list (VRRS)	Specifies additional attributes to include in VRRS accounting-on and accounting-off messages.

address (custom UDP probe)

To configure an IP address to which to send custom User Datagram Protocol (UDP) probes, use the **address** command in custom UDP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address*] [**routed**]

no address [*ip-address*] [**routed**]

Syntax Description

ip-address	(Optional) Destination IP address that is to respond to the custom UDP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: • Only one instance of a routed probe per server farm can run at any given time. • Outbound packets for a routed probe are routed directly to *ip-address*.

Defaults

If the custom UDP probe is associated with a firewall farm, you must specify an IP address.
If the custom UDP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a custom UDP probe named PROBE6, enters custom UDP probe configuration mode, and configures the probe to receive responses from IP address 13.13.13.13:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# address 13.13.13.13
```

Related Commands

Command	Description
ip slb probe custom udp	Configures a custom UDP probe name and enters custom UDP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

address (DNS probe)

To configure an IP address to which to send Domain Name System (DNS) probes, use the **address** command in DNS probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

ip-address	(Optional) Destination IP address that is to respond to the DNS probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: • Only one instance of a routed probe per server farm can run at any given time. • Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the DNS probe is associated with a firewall farm, you must specify an IP address.
If the DNS probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

DNS probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.1(12c)E	The **routed** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a DNS probe named PROBE4, enters DNS probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

Command	Description
ip slb probe dns	Configures a DNS probe name and enters DNS probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

address (HTTP probe)

To configure an IP address to which to send HTTP probes, use the **address** command in HTTP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

ip-address	(Optional) Destination IP address that is to respond to the HTTP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: • Only one instance of a routed probe per server farm can run at any given time. • Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the HTTP probe is associated with a firewall farm, you must specify an IP address.
If the HTTP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.1(12c)E	The **routed** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

address (ping probe)

To configure an IP address to which to send ping probes, use the **address** command in ping probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

ip-address	(Optional) Destination IP address that is to respond to the ping probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: • Only one instance of a routed probe per server farm can run at any given time. • Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the ping probe is associated with a firewall farm, you must specify an IP address.
If the ping probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

Ping probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.1(12c)E	The **routed** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a ping probe named PROBE1, enters ping probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE1 ping
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

Command	Description
ip slb probe ping	Configures a ping probe name and enters ping probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

address (TCP probe)

To configure an IP address to which to send TCP probes, use the **address** command in TCP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

ip-address	(Optional) Destination IP address that is to respond to the TCP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: • Only one instance of a routed probe per server farm can run at any given time. • Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the TCP probe is associated with a firewall farm, you must specify an IP address
If the TCP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.

Command Modes

TCP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.1(12c)E	The **routed** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a TCP probe named PROBE5, enters TCP probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE5 tcp
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

Command	Description
ip slb probe tcp	Configures a TCP probe name and enters TCP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

address (WSP probe)

To configure an IP address to which to send Wireless Session Protocol (WSP) probes, use the **address** command in WSP probe configuration mode. To restore the default settings, use the **no** form of this command.

address [*ip-address* [**routed**]]

no address [*ip-address* [**routed**]]

Syntax Description

ip-address	(Optional) Destination IP address that is to respond to the WSP probe.
routed	(Optional) Flags the probe as a routed probe, with the following considerations: • Only one instance of a routed probe per server farm can run at any given time. • Outbound packets for a routed probe are routed directly to the specified IP address.

Defaults

If the WSP probe is associated with a firewall farm, you must specify an IP address.
If the WSP probe is associated with a server farm, and you do not specify an IP address, the address is inherited from the server farm real servers.
In dispatched mode, the *ip-address* argument value is the same as the virtual server IP address. In directed Network Address Translation (NAT) mode, an IP address is unnecessary.

Command Modes

WSP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(5a)E	This command was introduced.
12.1(12c)E	The **routed** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a WSP probe named PROBE3, enters WSP probe configuration mode, and configures the probe to receive responses from IP address 10.1.10.1:

```
Router(config)# ip slb probe PROBE3 wsp
Router(config-slb-probe)# address 10.1.10.1
```

Related Commands

Command	Description
ip slb probe wsp	Configures a WSP probe name and enters WSP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

advertise

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

advertise [**active**]

no advertise [**active**]

Syntax Description

active	(Optional) Indicates that the host route is to be advertised only when the virtual IP address is available (that is, when there is at least one real server in OPERATIONAL, DFP_THROTTLED, or MAXCONNS state).

Defaults

The virtual server IP address is advertised. That is, a static route to the Null0 interface is installed for the virtual server IP addresses and it is added to the routing table.
If you do not specify the **active** keyword, the host route is advertised regardless of whether the virtual IP address is available.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

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

The **advertise** command does not affect virtual servers used for transparent web cache load balancing.

HTTP probes and route health injection require a route to the virtual server. The route is not used, but it must exist to enable the sockets code to verify that the destination can be reached, which in turn is essential for HTTP probes and route health injection to function correctly.

- For HTTP probes, the route can be either a host route (advertised by the virtual server) or a default route (specified using the **ip route 0.0.0.0 0.0.0.0** command, for example). If you specify either the **no advertise** or the **advertise active** command, you must specify a default route.
- For route health injection, the route must be a default route.

HTTP probes and route health injection can both use the same default route; you need not specify two unique default routes.

Examples

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

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# no advertise
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

agent

To identify a Dynamic Feedback Protocol (DFP) agent with which the IOS Server Load Balancing (IOS SLB) feature can initiate connections, use the **agent** command in SLB DFP configuration mode. To remove a DFP 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

ip-address	Agent IP address.
port	Agent TCP or User Datagram Protocol (UDP) port number.
timeout	(Optional) Time period, in seconds, during which the DFP manager must receive an update from the DFP agent. The valid range is 0 to 65535 seconds. The default is 0 seconds, which means there is no timeout.
retry-count	(Optional) Number of times the DFP manager attempts to establish the TCP connection to the DFP agent. The valid range is 0 to 65535 times. The default is 0 retries, which means there are infinite retries.
retry-interval	(Optional) Interval, in seconds, between retries. The valid range is 1 to 65535 seconds. 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 (config-slb-dfp)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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.

The password specified in the **ip slb dfp** command for the DFP manager must match the password specified in the **password** command for the DFP agent.

You can configure up to 1024 agents.

Examples

The following example sets the DFP password to Password1 (to match the DFP agent's password), sets the timeout to 360 seconds, enters DFP configuration mode, and enables IOS SLB to connect to the DFP agent with IP address 10.1.1.1 and port number 2221:

```
Router(config)# ip slb dfp password Password1 360
Router(config-slb-dfp)# agent 10.1.1.1 2221 30 0 10
```

Related Commands

Command	Description
ip dfp agent	Identifies a DFP agent subsystem and enters DFP agent configuration mode.
ip slb dfp	Configures DFP, supplies an optional password, and enters DFP configuration mode.

apn

To configure an ASCII regular expression string to be matched against the access point name (APN) for general packet radio service (GPRS) load balancing, use the **apn** command in SLB GTP map configuration mode. To delete the APN string, use the **no** form of this command.

apn *string*

no apn *string*

Syntax Description

string	ASCII regular expression string to be matched against the APN. For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the "Understanding Regular Expressions" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*: http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

Defaults

None

Command Modes

SLB GTP map configuration (config-slb-gtp-map)

Command History

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

Usage Guidelines

For a given IOS SLB GTP map, you can configure up to 100 **apn** commands. However, we recommend you configure no more than 10 **apn** commands per map.

Examples

The following example specifies that, for IOS SLB GTP map **2**, string **.cisco*** is to be matched against the APN:

```
Router(config)# ip slb map 2 gtp
Router(config-slb-gtp-map)# apn cisco*
```

Related Commands

Command	Description
ip slb map	Configures an IOS SLB protocol map and enters SLB map configuration mode.
show ip slb map	Displays information about IOS SLB protocol maps.

attribute list (VRRS)

To specify additional attributes to include in Virtual Router Redundancy Service (VRRS) accounting-on and accounting-off messages, use the **attribute list** command in VRRS configuration mode. To configure VRRS to send only default attributes in VRRS accounting messages, use the **no** form of this command.

attribute list *list-name*

no attribute list

Syntax Description

list-name	Specifies a AAA accounting list, as defined by the **aaa attribute list** global configuration command.

Command Default

Default attributes are sent in VRRS accounting messages.

Command Modes

VRRS configuration (config-vrrs)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **attribute list** (VRRS) command to specify additional attributes to be included in both VRRS accounting-on and accounting-off messages. Before configuring this command, define a list name using the **aaa attribute list** global configuration command. If you the enter a list name that is not defined in the **aaa attribute list** global configuration command, a warning message is displayed. However, this command is still accepted.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, vrrs
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Type
- Attribute 44 Acct-Session-Id

Examples

The following example configures VRRS to use the AAA accounting list named vrrp-1-attr:

```
Router(config)# aaa accounting vrrs default start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay "10"
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-name-1
```

```
Router(config-vrrs)# accounting delay 10
Router(config-vrrs)# attribute list vrrp-1-attr
```

Related Commands

Command	Description
aaa accounting vrrs	Enables AAA accounting of requested services for billing or security purposes when you use VRRS.
aaa attribute list	Defines a AAA attribute list locally on a router.
accounting delay (VRRS)	Specifies a delay time for sending accounting-off messages for VRRS.
accounting method (VRRS)	Enables VRRS accounting for a VRRP group.

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*]

Syntax Description

bind-id	(Optional) Bind ID number. The default bind ID is 0.

Defaults

The default bind ID is 0.

Command Modes

SLB server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure one bind ID on each **bindid** command.

The bind ID allows a single physical server to be bound to multiple virtual servers, and to 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. Dynamic Feedback Protocol (DFP) uses the bind ID to identify for which instance of the real server a given weight is specified.

In general packet radio service (GPRS) load balancing, bind IDs are not supported. Therefore do not use the **bindid** command in a GPRS load-balancing environment.

Examples

The following example configures bind ID 309:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# bindid 309
```

Related Commands

Command	Description
ip slb dfp	Configures DFP, supplies an optional password, and enters DFP configuration mode.
show ip slb serverfarms	Displays information about the IOS SLB server farms.

calling-station-id

To configure an ASCII regular expression string to be matched against the calling station ID attribute for RADIUS load balancing, use the **calling-station-id** command in SLB RADIUS map configuration mode. To delete the calling station ID match string, use the **no** form of this command.

calling-station-id *string*

no calling-station-id *string*

Syntax Description

string	ASCII regular expression string to be matched against the calling station ID attribute in the RADIUS payload. For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the "Understanding Regular Expressions" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*: http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

Defaults

None

Command Modes

SLB RADIUS map configuration (config-slb-radius-map)

Command History

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

Usage Guidelines

For a given IOS SLB RADIUS map, you can configure a single **calling-station-id** command or a single **username (IOS SLB)** command, but not both.

Examples

The following example specifies that, for IOS SLB RADIUS map **1**, string **.919*** is to be matched against the calling station ID attribute in the RADIUS payload:

```
Router(config)# ip slb map 1 radius
Router(config-slb-radius-map)# calling-station-id .919*
```

Related Commands

Command	Description
ip slb map	Configures an IOS SLB protocol map and enters SLB map configuration mode.
show ip slb map	Displays information about IOS SLB protocol maps.
username	Configures an ASCII regular expression string to be matched against the username attribute in the RADIUS payload.

carrier-delay (tracking)

To enable Enhanced Object Tracking (EOT) to consider the carrier-delay timer when tracking the status of an interface, use the **carrier-delay** command in tracking configuration mode. To disable EOT from considering the carrier-delay timer when tracking the status of an interface, use the **no** form of this command.

carrier-delay

no carrier-delay

Command Default

EOT does not consider the carrier-delay timer configured on an interface when tracking the status of the interface.

Command Modes

Tracking configuration (config-track)

Command History

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

Usage Guidelines

If a link fails, by default there is a two-second timer that must expire before an interface and the associated routes are declared as being down. If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the switch is not aware that a link-down event occurred. You can configure the **carrier-delay** *seconds* command in interface configuration mode to extend the timer up to 60 seconds.

When Enhanced Object Tracking (EOT) is configured on an interface, the tracking may detect the interface is down before a configured carrier-delay timer has expired. This is because EOT looks at the interface state and does not consider the carrier delay timer. Use the **carrier-delay** command in tracking configuration mode to enable tracking to consider the carrier-delay timer configured on an interface.

Examples

The following example shows how to configure the tracking module to wait for the interface carrier-delay timer to expire before notifying clients of a state change:

```
Router(config)# track 101 interface ethernet1/0 line-protocol
Router(config-track)# carrier-delay
```

Related Commands

Command	Description
carrier-delay	Sets the carrier delay on an interface.
show track	Displays information about objects that are tracked by the tracking process.
track interface	Configures an interface to be tracked and to enter tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

Command	Description
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.
track resolution	Specifies resolution parameters for a tracked object.
track rtr	Tracks the state of a Cisco IOS SLAs operation and enters tracking configuration mode.
track timer	Specifies the interval in which the tracking process polls the tracked object.

clear fm slb counters

To clear Feature Manager (FM) IOS Server Load Balancing (IOS SLB) counters, use the **clear fm slb counters** command in privileged EXEC mode.

clear fm slb {**inband** | **purge**} **counters**

Syntax Description

inband	Clears FM IOS SLB inband counters.
purge	Clears FM IOS SLB purge counters.

Defaults

FM IOS SLB counters are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.

Examples

The following example clears the FM IOS SLB inband counters:

```
Router# clear fm slb inband counters
```

Related Commands

Command	Description
show fm slb counters	Displays information about the Feature Manager (FM) IOS Server Load Balancing (IOS SLB) counters.

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**]

Syntax Description

checkpoint	(Optional) Clears the checkpointed database.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **clear ip accounting** EXEC command clears the active database and creates the checkpointed database.

Examples

The following example clears the active database when IP accounting is enabled:

```
Router# clear ip accounting
```

Related Commands

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

clear ip icmp rate-limit

To clear all Internet Control Message Protocol (ICMP) unreachable rate-limiting statistics or all statistics for a specified interface, use the **clear ip icmp rate-limit** command in privileged EXEC mode.

clear ip icmp rate-limit [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) Type of interface to be configured. Refer to the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4 for a list of valid interface types.
interface-number	(Optional) Port, connector, or interface card number. On Cisco 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

Defaults

All unreachable statistics for all devices are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following example shows how to clear all unreachable statistics on all interfaces:

```
Router# clear icmp rate-limit
```

Related Commands

Command	Description
ip icmp rate-limit unreachable	Limits the rate at which ICMP unreachable messages are generated for a destination.
show ip icmp rate-limit	Displays all ICMP unreachable rate-limiting statistics or all statistics for a specified interface.

clear ip sctp statistics

Note Effective with Cisco IOS Release 12.4(11)T, the **clear ip sctp statistics** command is replaced by the **clear sctp statistics** command. See the **clear sctp statistics** command for more information.

To clear statistics counts for Stream Control Transmission Protocol (SCTP) activity, use the **clear ip sctp statistics** command in privileged EXEC mode.

clear ip sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default value. If this command is not entered, statistics counts for SCTP activity continue to be logged.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.4(11)T	This command was replaced by the **clear sctp statistics** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command clears both individual and overall statistics.

Examples

The following command shows how to empty the buffer that holds SCTP statistics. No output is generated from this command.

```
Router# clear ip sctp statistics
```

Related Commands

Command	Description
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show ip sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays all currently defined SCTP instances.
show ip sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

clear ip slb connections

To clear the IP IOS Server Load Balancing (IOS SLB) connections, use the **clear ip slb connections** command in privileged EXEC mode.

clear ip slb connections [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*]

Syntax Description

firewallfarm *firewall-farm*	(Optional) Clears the IOS SLB connection database for the specified firewall farm.
serverfarm *server-farm*	(Optional) Clears the IOS SLB connection database for the specified server farm.
vserver *virtual-server*	(Optional) Clears the IOS SLB connection database for the specified virtual server.

Defaults

The IOS SLB connection database is cleared for all firewall farms, server farms, and virtual servers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)E	This command was introduced as part of the **clear ip slb** command.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(11b)E	This command was separated from the **clear ip slb** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In general packet radio service (GPRS) load balancing, the **clear ip slb connections** command clears connections, but does not clear sessions.

Examples

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

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

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

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

Related Commands

Command	Description
show ip slb conns	Displays information about active IOS SLB connections.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb serverfarms	Displays information about the IOS SLB server farms.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

clear ip slb counters

To clear the IP IOS Server Load Balancing (IOS SLB) counters, use the **clear ip slb counters** command in privileged EXEC mode.

clear ip slb counters [**kal-ap**]

Syntax Description

kal-ap	(Optional) clears only IP IOS SLB KeepAlive Application Protocol (KAL-AP) counters.

Defaults

IP IOS SLB counters are not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)E	This command was introduced as part of the **clear ip slb** command.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(11b)E	This command was separated from the **clear ip slb** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **kal-ap** keyword was added.

Examples

The following example clears the IP IOS SLB counters:

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

Related Commands

Command	Description
show ip slb stats	Displays IOS SLB statistics.

clear ip slb sessions

To clear the IP IOS Server Load Balancing (IOS SLB) sessions database, use the **clear ip slb sessions** command in privileged EXEC mode.

clear ip slb sessions [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*]

Syntax Description

firewallfarm *firewall-farm*	(Optional) Clears the IOS SLB session database for the specified firewall farm.
serverfarm *server-farm*	(Optional) Clears the IOS SLB session database for the specified server farm.
vserver *virtual-server*	(Optional) Clears the IOS SLB session database for the specified virtual server.

Defaults

If no optional keywords or arguments are specified, the IOS SLB sessions database is cleared of all firewall farms, server farms, and virtual servers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example clears the session database of server farm FARM1:

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

The following example clears the session database of virtual server VSERVER1:

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

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the IOS SLB firewall farms.
show ip slb sessions	Displays information about sessions handled by IOS SLB.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

clear ip slb sticky asn msid

To clear an entry from an IOS Server Load Balancing (IOS SLB) Access Service Network (ASN) Mobile Station ID (MSID) sticky database, use the **clear ip slb sticky asn msid** command in privileged EXEC mode.

clear ip slb sticky asn msid *msid*

Syntax Description

imsi	Clears the entry associated with the specified MSID from the IOS SLB ASN MSID sticky database.

Defaults

None

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

When you use this command to clear an entry from the IOS SLB ASN MSID sticky database, the session is not cleared; it lingers until it times out. (The session timeout is configured by using the **idle** command in SLB virtual server configuration mode; the default timeout is 60 seconds.) To clear the session manually, use the **clear ip slb sessions** command in privileged EXEC mode.

Examples

The following example clears the entry associated with MSID 001646013fc0 from the IOS SLB ASN MSID sticky database:

```
Router# clear ip slb sticky asn msid 001646013fc0
```

Related Commands

Command	Description
show ip slb sticky	Displays information about the IOS Server Load Balancing (IOS SLB) sticky database.

clear ip slb sticky gtp imsi

To clear entries from an IOS Server Load Balancing (IOS SLB) general packet radio service (GPRS) Tunneling Protocol (GTP) International Mobile Subscriber ID (IMSI) sticky database, use the **clear ip slb sticky gtp imsi** command in privileged EXEC mode.

clear ip slb sticky gtp imsi [**id** *imsi*]

Syntax Description

id *imsi*	Clears only the entry associated with the specified IMSI from the IOS SLB GTP IMSI sticky database.

Defaults

If you enter this command without the optional IMSI ID, all entries are cleared from the IOS SLB GTP IMSI sticky database.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you use this command to clear an entry from the IOS SLB GTP IMSI sticky database, the session is not cleared; it lingers until it times out. (The session timeout is configured by using the **idle** command in SLB virtual server configuration mode; the default timeout is 30 seconds.) If the same user tries to create a new Packet Data Protocol (PDP) context before the session times out, using the same Network Service Access Point Identifier (NSAPI) but a different access point name (APN), IOS SLB forwards the request to the old server farm, even though the new APN should lead to a different server farm. To avoid this problem, clear the session manually by using the **clear ip slb sessions** command in privileged EXEC mode.

Examples

The following example clears all entries from the IOS SLB GTP IMSI sticky database:

```
Router# clear ip slb sticky gtp imsi
```

Related Commands

Command	Description
show ip slb sticky	Displays information about the IOS Server Load Balancing (IOS SLB) sticky database.

clear ip slb sticky radius

To clear entries from a IOS Server Load Balancing (IOS SLB) RADIUS sticky database, use the **clear ip slb sticky radius** command in privileged EXEC mode.

clear ip slb sticky radius {**calling-station-id** [**id** *string*] | **framed-ip** [*framed-ip* [*netmask*]]}

Syntax Description

calling-station-id	Clears entries from the IOS SLB RADIUS calling-station-ID sticky database.
id *string*	(Optional) Calling station ID of the entry to be cleared.
framed-ip	Clears entries from the IOS SLB RADIUS framed-IP sticky database.
framed-ip	(Optional) Framed-IP address of entries to be cleared.
netmask	(Optional) Subnet mask specifying a range of entries to be cleared.

Defaults

If no optional arguments are specified, all entries are cleared from the IOS SLB RADIUS calling-station-ID sticky database or framed-IP sticky database.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)ZA5	The **calling-station-id** and **id** keywords and *string* argument were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you use this command to clear an entry from the IOS SLB RADIUS calling-station-ID sticky database, the session is not cleared; it lingers until it times out. (The session timeout is configured by using the **idle** command in SLB virtual server configuration mode; the default timeout is 30 seconds.) If the same user tries to create a new Packet Data Protocol (PDP) context before the session times out, using the same Network Service Access Point Identifier (NSAPI) but a different access point name (APN), IOS SLB forwards the request to the old server farm, even though the new APN should lead to a different server farm. To avoid this problem, clear the session manually by using the **clear ip slb sessions** command in privileged EXEC mode.

Examples

The following example clears all entries from the IOS SLB RADIUS framed-IP sticky database:

```
Router# clear ip slb sticky radius framed-ip
```

Related Commands

Command	Description
show ip slb sticky	Displays information about the IOS SLB sticky database.

clear ip tcp header-compression

To clear the TCP, UDP, and IP header-compression statistics, use the **clear ip tcp header-compression** command in privileged EXEC mode.

clear ip tcp header-compression *interface-type interface-number*

Syntax Description

interface-number	Specifies the interface type.
interface-number	Specifies the interface number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to clear the header-compression statistics for an ATM interface:

```
Router# clear  ip tcp header-compression ATM2/0
```

Related Commands

Command	Description
show ip tcp header-compression	Displays statistics about TCP header compression.

clear ip traffic

To clear the global or system-wide IP traffic statistics for one or more interfaces, use the **clear ip traffic** command in privileged EXEC mode.

clear ip traffic [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Clears the global or system-wide IP traffic statistics for a specific interface. If the **interface** keyword is used, the *type* and *number* arguments are required.

Command Default

Using the **clear ip traffic** command with no keywords or arguments clears the global or system-wide IP traffic statistics for all interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.1S	This command was modified to include the optional **interface** keyword and associated *type* and *number* arguments. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293: *Management Information Base for the Internet Protocol (IP)*.

Usage Guidelines

Using the **clear ip traffic** command with the optional **interface** keyword clears the ipIfStatsTable counters displayed for the specified interface and also clears the counters displayed by the **show ip traffic interface** command.

Examples

The following example clears the global or system-wide IP traffic statistics on all interfaces:

```
Router# clear ip traffic
```

Related Commands

Command	Description
show ip traffic	Displays the global or system-wide IP traffic statistics for one or more interfaces.

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 privileged EXEC mode.

clear ip wccp [**vrf** *vrf-name* {**web-cache** | *service-number*}] [**web-cache** | *service-number*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	(Optional) Directs the router to remove statistics for the web cache service.
service-number	(Optional) Number of the cache service to be removed. The number can be from 0 to 99.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1CA	This command was introduced for Cisco 7200 and 7500 platforms.
11.2P	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 **web-cache** keyword and the *service-number* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

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.

Use the **clear ip wccp** command to clear the WCCP counters for all WCCP services in all VRFs.

Use the **clear ip wccp vrf** *vrf-name* {**web-cache** | **service-number**} command to clear the WCCP counters for the specific WCCP service in the specified VRF.

Examples

The following example shows how to clear all statistics associated with the web cache service:

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

Related Commands

Command	Description
clear platform software wccp	Clears WCCPv2 statistics on the Cisco ASR 1000 Series Routers.
ip wccp	Enables support of the specified WCCP service for participation in a service group.
show ip wccp	Displays global statistics related to the WCCP.

clear mls acl counters

To clear the multilayer switching (MLS) access control list (ACL) counters, use the **clear mls acl counters** command in privileged EXEC mode.

clear mls acl counters {**all** [**module** *num*] | **interface** *interface interface-number* [**loopback** *interface-number* | **null** *interface-number* | **port-channel** *number* | **vlan** *vlan-id*]}

Syntax Description

all	Clears all the MLS ACL counters for all interfaces.
module *num*	(Optional) Clears all the MLS ACL counters for the specified DFC.
interface *interface*	Clears counters that are associated with the specified interface; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
interface-number	Module and port number; see the "Usage Guidelines" section for valid values.
loopback *interface-number*	(Optional) Specifies the loopback interface; valid values are from 0 to 2147483647.
null *interface-number*	(Optional) Specifies the null interface; the valid value is **0**.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The valid values for *interface* include the **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on Cisco 7600 series routers that are configured with a WS-F6K-DFC3B-XL, release 2.1 and later.

If you enter the **clear mls acl counters all module** *num* command, all the MLS ACL counters for the specified DFC only are cleared. If you enter the **clear mls acl counters all** command without entering the **module** *num* keyword and argument, all the MLS ACL counters for only the non-DFC modules and the supervisor engines are cleared.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows how to reset the MLS ACL counters in all interfaces:

```
Router# clear mls acl counters all
```

Related Commands

Command	Description
show tcam interface	Displays information about the interface-based TCAM.

clear platform software wccp

To clear Web Cache Communication Protocol version 2 statistics on the Cisco ASR 1000 Series Routers, use the **clear platform software wccp** command in privileged EXEC mode.

clear platform software wccp {*slot* [**active** | **standby**] **statistics**} | {**counters** | **statistics**}

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: • **F0**—Embedded Service Processor slot 0 • **F1**—Embedded Service Processor slot 1 • **FP**—Embedded Service Processor • **R0**—Route Processor slot 0 • **R1**—Route Processor slot 1 • **RP**—Route Processor
active	Clears active instances.
standby	Clears standby instances.
statistics	Clears statistics counters.
counters	Clears packet processing counters.

Command Default

WCCPv2 statistics are not cleared.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to clear WCCPv2 statistics on Embedded-Service-Processor slot 0:

```
Router# clear platform software wccp F0 statistics
```

Related Commands

Command	Description
clear ip wccp	Removes WCCP statistics (counts) maintained on the router for a particular service.

clear sctp statistics

To clear statistics counts for Stream Control Transmission Protocol (SCTP) activity, use the **clear sctp statistics** command in privileged EXEC mode.

clear sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default value. If this command is not entered, statistics counts for SCTP activity continue to be logged.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **clear ip sctp statistics** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command clears both individual and overall statistics.

Examples

The following command shows how to empty the buffer that holds SCTP statistics. No output is generated from this command.

```
Router# clear sctp statistics
```

Related Commands

Command	Description
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instances	Displays all currently defined SCTP instances.
show sctp statistics	Displays overall statistics counts for SCTP.

Command	Description
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

clear sockets

To close all IP sockets and clear the underlying transport connections and data structures, use the **clear sockets** command in privileged EXEC mode.

clear sockets *process-id*

Syntax Description

process-id	Identifier of the IP process to be cleared.

Command Default

IP socket information is not cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Using this command results in an abortive close for TCP connections and Stream Control Transfer Protocol (SCTP) associations. When this command is entered, TCP connections abort by sending an RST (restore) and SCTP associations abort by sending an ABORT signal to the peer.

Use the **show processes** command to display the list of running processes and their associated process IDs.

You can use the **show sockets detail** command to confirm all open sockets have been cleared.

Examples

The following example shows how to close all sockets for IP process 35:

```
Router# clear sockets 35

All sockets (TCP, UDP and SCTP) for this process will be cleared.
Do you want to proceed? [yes/no]: y
Cleared sockets for PID 35
```

Related Commands

Command	Description
show processes	Displays information about the active processes.
show sockets	Displays IP socket information.
show udp	Displays IP socket information about UDP processes.

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 (#)

Command History

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

Examples

The following example clears all TCP statistics:

```
Router# clear tcp statistics
```

Related Commands

Command	Description
show tcp statistics	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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

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

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

Related Commands

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

client (virtual server)

To define which clients are allowed to use the virtual server, use the **client** command in Server Load Balancing (SLB) virtual server configuration mode. To remove a client definition from the SLB configuration, use the **no** form of this command.

client {*ipv4-address netmask* [**exclude**] | **gtp carrier-code** [*code*]}

no client {*ipv4-address netmask* [**exclude**] | **gtp carrier-code** [*code*]}

Syntax Description

ipv4-address	Client IPv4 address. The default is 0.0.0.0 (all clients).
netmask	Client IPv4 network mask. The default is 0.0.0.0 (all subnets).
exclude	(Optional) Ignores connections initiated by the client IPv4 address from the load-balancing scheme.
gtp carrier-code	For general packet radio service (GPRS) Tunneling Protocol (GTP) cause code inspection, configures the virtual server to accept Packet Data Protocol (PDP) context creates only from the specified International Mobile Subscriber Identity (IMSI) carrier code.
code	(Optional) For GTP cause code inspection, identifies the IMSI carrier code from which this virtual server is to accept PDP context creates. The code has the format: **mcc** *mcc-code* **mnc** *mnc-code* where: • *mcc-code* is the Mobile Country Code (MCC) • *mnc-code* is the Mobile Network Code (MNC) If you do not specify a *code*, the virtual server accepts PDP context creates from any IMSI carrier code.

Command Default

The default client IPv4 address is 0.0.0.0 (all clients).
The default client IPv4 network mask is 0.0.0.0 (all subnets).
Taken together, the default is client 0.0.0.0 0.0.0.0 (allows all clients on all subnets to use the virtual server).
If you specify **gtp carrier-code** and you do not specify a code, the virtual server accepts PDP context creates from any IMSI carrier code.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(1)E	The **exclude** keyword was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp carrier-code** keyword and *code* argument were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can use more than one client command to define more than one client.

The *netmask* value is applied to the source IPv4 address of incoming connections. The result must match the *ipv4-address* value for the client to be allowed to use the virtual server.

If you configure probes in your network, you must also do one of the following:

- Configure the **exclude** keyword on the **client** command on the virtual server to exclude connections initiated by the client IPv4 address from the load-balancing scheme.
- Configure IPv4 addresses on the IOS SLB device that are Layer 3-adjacent to the real servers used by the virtual server.

Configure separate **client** commands to specify the clients that can use the virtual server, and to specify the IMSI carrier code from which the virtual server is to accept PDP context creates.

Dual-stack support for GTP load balancing does not support this command.

Examples

The following example allows clients from only 10.4.4.0 access to the virtual server:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# client 10.4.4.0 255.255.255.0
```

Related Commands

Command	Description
show ip slb vserver	Displays information about the virtual servers defined to IOS SLB.
virtual (virtual server)	Configures the virtual server attributes.

credentials (HTTP probe)

To configure basic authentication values for the HTTP IOS Server Load Balancing (IOS SLB) probe, use the **credentials** command in HTTP probe configuration mode. To remove a **credentials** configuration, use the **no** form of this command.

credentials *username* [*password*]

no credentials *username* [*password*]

Syntax Description

username	Authentication username of the HTTP probe header. The character string is limited to 15 characters.
password	(Optional) Authentication password of the HTTP probe header. The character string is limited to 15 characters.

Defaults

Basic authentication values for the HTTP IOS SLB probe are not configured.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP probe configuration mode, sets the HTTP authentication to username Username1, and sets the password to develop:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# credentials Username1 develop
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

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

delay	Default delay value.
object *object-number*	Default object for the list. The *object-number* argument has a valid range of 1 to 1000.
threshold percentage	Default threshold percentage.

Command Default

No default values for a track list are set.

Command Modes

Tracking configuration (config-track)

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.
15.1(3)T	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

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

```
Router(config)# track 3 list
Router(config-track)# default threshold percentage
```

Related Commands

Command	Description
show track	Displays tracking information.
threshold weight	Specifies a threshold weight for a tracked list.

Command	Description
track list threshold percentage	Tracks a list of objects as to the up and down object states using a threshold percentage.
track list threshold weight	Tracks a list of objects as to the up and down object states using a threshold weight.

default-state

To set the default state for a stub object, use the **default-state** command in tracking configuration mode. To reset the default state to its internal default state, use the **no** form of this command.

default-state {**up** | **down**}

no default-state {**up** | **down**}

Syntax Description

up	Sets the current default state of a stub object to up.
down	Sets the current default state of a stub object to down.

Command Default

Internal default state is the default.

Command Modes

Tracking configuration (config-track)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **default-state** command to set the default state of a stub object that has been created by the **track stub** command. The stub object can be tracked and manipulated by an external process, Embedded Event Manager (EEM).

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

Examples

The following example shows how to create a stub object and configure a default state for the stub object:

```
track 2 stub
 default-state up
```

Related Commands

Command	Description
show track	Displays tracking information.
track stub	Creates a stub object to be tracked.

delay (firewall farm TCP protocol)

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

delay *duration*

no delay

Syntax Description

duration	Delay timer duration in seconds. The valid range is 1 to 600 seconds. The default value is 10 seconds.

Defaults

The default duration is 10 seconds.

Command Modes

Firewall farm TCP protocol configuration (config-slb-fw-tcp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

Examples

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

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# delay 30
```

Related Commands

Command	Description
protocol tcp	Enters firewall farm TCP protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.

delay (tracking)

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

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

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

Syntax Description

up	Time to delay the notification of an up event.
down	Time to delay the notification of a down event.
seconds	Delay value, in seconds. The range is from 0 to 180. The default is 0.

Defaults

No delay time is configured for tracking.

Command Modes

Tracking configuration (config-track)

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)B.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 a down event of the tracked object to the client process is set to 30 seconds.

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

delay (virtual server)

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

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

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

Syntax Description

duration	Delay timer duration for TCP connection context, in seconds. The valid range is 1 to 600 seconds. The default value is 10 seconds.
radius framed-ip *duration*	Delay timer for RADIUS framed-ip sticky database, in seconds. The valid range is 1 to 43200 seconds. The default value is 10 seconds.

Defaults

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

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(18)E	The **radius** and **framed-ip** keywords and the *duration* argument were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

expect

To configure a status code or regular expression to expect information from the HTTP probe, use the **expect** command in HTTP probe configuration mode. To restore the default settings, use the **no** form of this command.

expect [**status** *status-code*] [**regex** *expression*]

no expect [**status** *status-code*] [**regex** *expression*]

Syntax Description

status *status-code*	(Optional) Configures the expected HTTP status code. The valid range is 100 to 599. The default expected status code is 200.
regex *expression*	(Optional) Configures the regular expression expected in the HTTP response. For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the "Understanding Regular Expressions" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*: http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

Defaults

The default expected status code is 200.
There is no default expected regular expression.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(3a)E	The **regex** keyword and *expression* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **expect** command configures the expected status code or regular expression to be received from the servers. A real server is considered to have failed and is taken out of service if any of the following events occurs:

- A status number other than the expected one is received.
- The expected regular expression is not received in the first 2920 bytes of probe output. (IOS Server Load Balancing [IOS SLB] searches only the first 2920 bytes for the expected status code or regular expression.)
- The server fails to respond.

For IOS SLB firewall load balancing, configure the HTTP probe to expect status code 40l.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP configuration mode, and configures the HTTP probe to expect the status code 40l and the regular expression Copyright:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# expect status 401 regex Copyright
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

failaction (firewall farm)

To configure the IOS Server Load Balancing (IOS SLB) feature's behavior when a firewall fails, use the **failaction** command in firewall farm configuration mode.

failaction purge

Syntax Description

purge	Enables IOS SLB to automatically remove connections to failed firewalls from the connection database even if the idle timers have not expired.

Defaults

If you do not specify the **failaction** command, IOS SLB does not automatically remove connections to failed firewalls.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is useful for applications that do not rotate the source port (such as Internet Key Exchange [IKE]), and for protocols that do not have ports to differentiate flows (such as Encapsulation Security Payload [ESP]).

Examples

In the following example, IOS SLB removes all connections to failed firewalls in firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# failaction purge
```

failaction (server farm)

To configure IOS Server Load Balancing (IOS SLB) feature's behavior when a real server fails, use the **failaction** command in server farm configuration mode. To restore the default settings, use the **no** form of this command.

failaction {**purge** | **asn purge** | **gtp purge** | **radius reassign**}

no failaction {**purge** | **asn purge** | **gtp purge** | **radius reassign**}

Syntax Description

purge	Enables IOS SLB to automatically remove connections to failed real servers from the connection database even if the idle timers have not expired.
asn purge	Enables IOS SLB to automatically remove objects associated with failed real servers from the Access Service Network (ASN) sticky database, even if the idle timers have not expired.
gtp purge	Enables IOS SLB to automatically remove objects associated with failed real servers from the general packet radio service (GPRS) Tunneling Protocol (GTP) International Mobile Subscriber ID (IMSI) sticky database, even if the idle timers have not expired.
radius reassign	Enables IOS SLB to automatically reassign to a new real server RADIUS sticky objects that are destined for a failed real server.

Defaults

If you do not specify the **failaction** command, IOS SLB does not perform the following actions:

- Remove connections to failed real servers
- Remove connections to objects associated with failed real servers
- Remove ASN or GPRS sticky objects (IOS SLB continues to assign new session requests to the failed real servers)
- Reassign RADIUS sticky objects

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.1(11b)E	The **radius reassign** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	The **gtp purge** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	The **asn purge** keywords were added.

Usage Guidelines

This command is useful for applications that do not rotate the source port (such as Internet Key Exchange [IKE]), and for protocols that do not have ports to differentiate flows (such as Encapsulation Security Payload [ESP]).

You can specify **no failaction purge**, but it has no effect on the connection database.

If you specify **failaction radius reassign**, IOS SLB reassigns RADIUS sticky objects without seeing any new RADIUS messages. The assumption is that, in the event of a failure, the RADIUS proxy gateways can handle user flows without seeing the RADIUS messages. If the RADIUS proxy gateways cannot do so, do not specify the **failaction radius reassign** command.

Examples

In the following example, IOS SLB removes all connections to failed real servers in server farm PUBLIC:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# failaction purge
```

faildetect (custom UDP probe)

To specify the number of consecutive unacknowledged custom User Datagram Protocol (UDP) probes that constitute failure of the real server, use the **faildetect** command in custom UDP probe configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect *number-of-probes*

no faildetect

Syntax Description

number-of-probes	Number of consecutive unacknowledged custom UDP probes allowed before a real server is considered to have failed. Valid range is 1 to 65535. The default value is one (1) unacknowledged custom UDP probe.

Defaults

The default value is one (1) unacknowledged probe.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

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

Examples

In the following example the unacknowledged custom UDP probe threshold is set to 16:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# faildetect 16
```

Related Commands

Command	Description
ip slb probe custom udp	Configures a custom User Datagram Protocol (UDP) probe name and enters custom UDP probe configuration mode.
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

faildetect (DNS probe)

To specify the conditions that indicate a server failure, use the **faildetect** command in DNS probe configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect *number-of-probes*

no faildetect

Syntax Description

number-of-probes	Number of consecutive unacknowledged Domain Name System (DNS) probes allowed before a real server is considered to have failed. Valid range is 1 to 65535. The default value is three (3) unacknowledged DNS probes.

Defaults

The default value is three (3) unacknowledged DNS probes.

Command Modes

DNS probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example the unacknowledged DNS probe threshold is set to 16:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# faildetect 16
```

Related Commands

Command	Description
ip slb probe dns	Configures a Domain Name System (DNS) probe name and enters DNS probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

faildetect (ping probe)

To specify the conditions that indicate a server failure, use the **faildetect** command in ping probe configuration mode. To restore the default values that indicate a server failure, use the **no** form of this command.

faildetect *number-of-pings*

no faildetect

Syntax Description

number-of-pings	Number of consecutive unacknowledged pings allowed before a real server is considered to have failed. Valid range is 1 to 65535. The default is ten (10) unacknowledged pings.

Defaults

The default value is ten (10) unacknowledged pings.

Command Modes

Ping probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example the unacknowledged ping threshold is set to 16:

```
Router(config)# ip slb probe PROBE1 ping
Router(config-slb-probe)# faildetect 16
```

Related Commands

Command	Description
ip slb probe ping	Configures a ping probe name and enters ping probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

faildetect inband (real server)

To enable automatic server failure detection, use the **faildetect inband** command in real server configuration mode. To disable automatic server failure detection, use the **no** form of this command.

faildetect inband

no faildetect inband

Syntax Description

This command has no arguments or keywords.

Defaults

Automatic server failure detection is enabled.

Command Modes

Real server configuration (config-slb-real)

Command History

Release	Modification
12.2(14)ZA4	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you have configured all-port virtual servers (that is, virtual servers that accept flows destined for all ports except GTP ports), flows can be passed to servers for which no application port exists. When the servers reject these flows, Cisco IOS SLB might fail the servers and remove them from load balancing. This situation can also occur in slow-to-respond AAA servers in RADIUS load-balancing environments. To prevent this situation, you can disable automatic server failure detection using the **no faildetect inband** command.

Note If you disable automatic server failure detection using the **no faildetect inband** command, Cisco strongly recommends that you configure one or more probes.

If you specify the **no faildetect inband** command, the **faildetect numconns** command is ignored, if specified.

Examples

In the following example, automatic server failure detection is disabled:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# no faildetect inband
```

Related Commands

Command	Description
faildetect numconns (real server)	Specifies the conditions that indicate a real server failure.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

faildetect numconns (real server)

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

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

no faildetect numconns *number-of-conns* [**numclients** *number-of-clients*]

Syntax Description

number-of-conns	Number of consecutive connection failures allowed before IOS Server Load Balancing (IOS SLB) fails the real server. The valid range is 1 to 255. The default value is 8.
numclients *number-of-clients*	(Optional) Number of unique client IP addresses that can experience connection failures before IOS SLB fails the real server. The valid range is 1 to 8. The default value is 2. If there is only one client in your network (for example, one serving GPRS support node [SGSN] in a general packet radio service [GPRS] load-balancing environment), then you must specify **numclients 1**. In RADIUS load balancing, for automatic session-based failure detection, specify **numclients 1**.

Defaults

If you do not specify the **faildetect numconns** command, the default value of the connection failure threshold is 8.
If you specify the **faildetect numconns** command but do not specify the **numclients** keyword, the default value of the client connection failure threshold is 2.

Command Modes

SLB real server configuration (config-slb-real)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(9)E	This command was modified to support GPRS load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you specify the **no faildetect inband** command, the **faildetect numconns** command is ignored, if specified.

IOS SLB does not fail the real server until both of the following conditions are met:

- There have been *number-of-conns* consecutive connection failures.
- There have been *number-of-clients* unique client connection failures.

That is, there can be many consecutive connection failures, but until there have also been *number-of-clients* unique client connection failures, IOS SLB does not fail the real server.

Similarly, there can be many unique client connection failures, but until there have also been *number-of-conns* consecutive connection failures, IOS SLB does not fail the real server.

GPRS load balancing has the following features:

- The **numconns** keyword specifies the number of consecutive Create Packet Data Protocol (PDP) requests allowed before IOS SLB fails the gateway GPRS support node (GGSN).
- The **numclients** keyword specifies the number of unique client Create PDP request failures allowed before IOS SLB fails the GGSN.

Examples

In the following example, the **numconns** keyword is set to 10 and the **numclients** keyword is set to 3:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# faildetect numconns 10 numclients 3
```

With those settings, IOS SLB will not fail the real server until there have been ten (10) consecutive connection failures and there have been three (3) unique client connection failures.

Related Commands

Command	Description
faildetect inband (real server)	Enables automatic server failure detection.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

farm-weight

To specify a weight to be used by the IOS SLB KeepAlive Application Protocol (KAL-AP) agent when calculating the load value for a server farm, use the **farm-weight** command in server farm configuration mode. To restore the default weight value, use the **no** form of this command.

farm-weight *setting*

no farm-weight

Syntax Description

setting	Weight setting to be used by the KAL-AP agent. Valid settings range from 1 to 4294967295.

Defaults

If you do not configure a KAL-AP farm weight, IOS SLB calculates a relative weight.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

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

Usage Guidelines

Configuring a **farm-weight** enables KAL-AP to calculate loads more accurately when load balancing in a global server load balancing (GSLB) environment.

For best results, configure a **farm-weight** that is equal to the sum of the maximum DFP weights for the real servers in the server farm. (The maximum DFP weight for a real server is configured using the **gprs dfp max-weight** command in global configuration mode.) For example, if there are three real servers in a server farm, configured with maximum DFP weights of 100, 50, and 50, then configure a **farm-weight** of 200 (that is, 100 + 50 + 50). If a real server is added to or removed from the server farm, you must adjust the **farm-weight** accordingly.

Examples

The following example specifies that a weight of 16 is to be used by the KAL-AP agent when calculating the load value for a server farm:

```
Router(config-slb-sfarm)# farm-weight 16
```

Related Commands

Command	Description
gprs dfp max-weight	Specifies the maximum weight sent to a DFP manager by a Gateway GPRS Support Node (GGSN) acting as a DFP agent.
ip slb capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.
ip slb serverfarm	Identifies a server farm and enter SLB server farm configuration mode.

forwarding-agent

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

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

no forwarding-agent

Syntax Description

port-number	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.
password	(Optional) Text password used for generating the MD5 digest.
timeout	(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 (config-casa)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

```
forwarding-agent 1637
```

Related Commands

Command	Description
show ip casa oper	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

group-number	GLBP group number in the range from 0 to 1023.
text *string*	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
md5	Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key string cannot exceed 100 characters in length. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
7	(Optional) Encrypted key.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No authentication of GLBP messages occurs.

Command Modes

Interface configuration (config-if)

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 **md5** keyword and associated parameters were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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 interoperation. 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:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# 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:

```
Router(config)# key chain AuthenticateGLBP
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
service password-encryption	Encrypts passwords.

glbp client-cache maximum

To enable the Gateway Load Balancing Protocol (GLBP) client cache, use the **glbp client-cache** command in interface configuration mode. To disable a GLBP client cache, use the **no** form of this command.

glbp *group* **client-cache maximum** *number* [**timeout** *minutes*]

no glbp *group-number* **client-cache maximum** *number* [**timeout** *minutes*]

Syntax Description

group	GLBP group number in the range from 0 to 1023.
number	Specifies the maximum number of clients the cache will hold for this GLBP group. The range is from 8 to 2000.
timeout *minutes*	(Optional) The maximum amount of time, in minutes, a client entry can stay in the GLBP client cache after the client information was last updated. The range is from 1 to 1440.

Command Default

The GLBP client cache is disabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command enables a GLBP client cache on a single group only. To enable the client cache on multiple GLBP groups, you must apply this command to each group for which a client cache is required.

You must specify a maximum number of clients that the client cache will hold for a GLBP group to limit the size of the cache. If a GLBP client cache already exists when this command is entered and there are already more clients in the cache than the required number, all of the existing cache entries are discarded.

If you enter the **no** form of this command when there are already client entries in the cache, all of the client entries are discarded before the GLBP client cache is disabled.



Note For IPv4 networks, Cisco recommends setting a GLBP client cache timeout value that is slightly longer than the maximum expected end-host Address Resolution Protocol (ARP) cache timeout value.

Examples

The following example shows how to enable a GLBP client cache with a maximum of 1200 clients:

```
Router(config-if)# glbp 10 client-cache maximum 1200 timeout 245
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp forwarder preempt

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

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

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

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp ip

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

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

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

Syntax Description

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

Command Default

GLBP is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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

Command	Description
show glbp	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

group	GLBP group number in the range from 0 to 1023.
host-dependent	(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.
round-robin	(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.
weighted	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

Command Default

The round-robin method is the default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T2	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.0(1)M1	This command was modified. When the **no** form of this command is configured, if the AVG does not have an Active Virtual Forwarder (AVF), it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.
15.1(2)T	This command was modified. When the **no** form of this command is configured, if the AVG does not have an AVF, it preferentially replies to ARP requests with the MAC address of the first listening virtual forwarder.

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:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip 10.21.8.10
Router(config-if)# glbp 10 load-balancing host-dependent
```

Related Commands

Command	Description
show glbp	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

group-number	GLBP group number. Range is from 0 to 1023.
group-name	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 (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
glbp authentication	Configures an authentication string for the GLBP.
glbp forwarder preempt	Configures a router to take over as AVF for a GLBP group if it has higher priority than the current AVF.
glbp ip	Activates GLBP.
glbp load-balancing	Specifies the load-balancing method used by the AVG of GLBP.

Command	Description
glbp preempt	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
glbp priority	Sets the priority level of the gateway within a GLBP group.
glbp timers	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.
glbp timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
glbp weighting	Specifies the initial weighting value of the GLBP gateway.
glbp weighting track	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
show glbp	Displays GLBP information.
track	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 function, use the **no** form of this command.

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

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

Syntax Description

group	GLBP group number in the range from 0 to 1023.
delay minimum *seconds*	(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.

Command Default

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 (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
glbp ip	Enables GLBP.
glbp priority	Sets the priority level of the router within a GLBP group.

glbp priority

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

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

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

Syntax Description

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

Command Default

The GLBP virtual gateway preemptive scheme is disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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
glbp ip	Enables GLBP.
glbp preempt	Configures a router to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

glbp sso

To enable Gateway Load Balancing Protocol (GLBP) support of Stateful Switchover (SSO) if it has been disabled, use the **glbp sso** command in global configuration mode. To disable GLBP support of SSO, use the **no** form of this command.

glbp sso

no glbp sso

Syntax Description

This command has no arguments or keywords.

Command Default

GLBP Support for SSO is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to enable GLBP support of SSO if it has been manually disabled by the **no glbp sso** command.

Examples

The following example show how to disable GLBP support of SSO:

```
Router(config)# no glbp sso
```

Related Commands

Command	Description
debug glbp events	Displays debugging messages about GLBP events.
show glbp	Displays GLBP information.

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

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

Defaults

hellotime: 3 seconds
holdtime: 10 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 ip
Router(config-if)# glbp 10 timers 5 18
```

Related Commands

Command	Description
glbp ip	Activates GLBP.
show glbp	Displays GLBP information.

glbp timers redirect

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

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

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

Syntax Description

group	GLBP group number in the range from 0 to 1023.
redirect	The redirect timer interval in the range from 0 to 3600 seconds. The default is 600 seconds (10 minutes). **Note** The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.
timeout	The time interval, in the range from 600 to 64,800 seconds, before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Command Default

redirect: 600 seconds (10 minutes)
timeout: 14,400 seconds (4 hours)

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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.

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 is still given out in Address Resolution Protocol (ARP) replies, but the forwarding task is handled by another router in the GLBP group.



Note The zero value for the *redirect* argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and, if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a router fails, new hosts continue to be assigned to the failed router instead of being redirected to the backup.

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.

Examples

The following example shows the commands used to configure GLBP group 1 on Fast Ethernet interface 0/0 with a redirect timer of 1800 seconds (30 minutes) and timeout interval of 28,800 seconds (8 hours):

```
Router# config terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# glbp 1 timers redirect 1800 28800
```

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

group	GLBP group number in the range from 0 to 1023.
maximum	Maximum weighting value in the range from 1 to 254. Default value is 100.
lower *lower*	(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
upper *upper*	(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.

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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

Command	Description
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
track	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

group	GLBP group number in the range from 0 to 1023.
object-number	Object number representing an item to be tracked. The valid range is 1 to 1000. Use the **track** command to configure the tracked object.
decrement *value*	(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.

Command Default

Objects are not tracked for GLBP weighting changes.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

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.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

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.

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting track 1
Router(config-if)# glbp 10 weighting track 2 decrement 5
```

Related Commands

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

gtp notification cac

To limit the number of times IOS SLB can reassign a session to a new real server for GGSN-IOS SLB messaging, use the **gtp notification cac** command in virtual server configuration mode. To restore the default limit, use the **no** form of this command.

gtp notification cac [*reassign-count*]

no gtp notification cac

Syntax Description

reassign-count	(Optional) Number of times IOS SLB can reassign a session to a new real server. That is, the number of times that IOS SLB can reassign a rejected Create PDP Context to a new real GGSN. The valid range is 1 to 20 reassignments. The default setting is 2 reassignments (that is, the initial real server assignment and 2 additional reassignments).

Defaults

The default is 2 reassignments (that is, the initial real server assignment and 2 additional reassignments).

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(17d)SXB1	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that IOS SLB can reassign a session up to 5 times:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# gtp notification cac 5
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

gtp session (virtual server)

To enable IOS SLB to create general packet radio service (GPRS) Tunneling Protocol (GTP) load-balancing sessions, use the **gtp session** command in SLB virtual server configuration mode. To disable the creation of GTP sessions by IOS SLB, (the sticky-only load-balancing solution), use the **no** form of this command.

gtp session

no gtp session

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB creates GTP load-balancing sessions.
Sticky-only load-balancing is disabled.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

Sticky-only load balancing is supported for all versions of GTP.

If sticky-only load balancing (**no gtp session**) is enabled for GTP:

- IOS SLB load-balances GTP Packet Data Protocol (PDP) create requests based on the sticky objects in the GTP International Mobile Subscriber ID (IMSI) sticky database.
- Sticky connections must also be enabled for the virtual server, using the **sticky (virtual server)** command.
- Automatic server failure detection (the **faildetect inband** command) is not supported. Instead, use probes to detect real server failures.

Examples

The following example specifies that sticky-only load balancing is to be used for GTP:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# no gtp session
```

Related Commands

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

gw port (virtual server)

To specify the port that the Cisco Broadband Wireless Gateway (BWG) is to use to communicate with IOS SLB, use the **gw port** command in SLB virtual server configuration mode. To restore the default settings, use the **no** form of this command.

gw port *port*

no gw port *port*

Syntax Description

port	Port number used by the Cisco BWG to communicate with IOS SLB. This port number must be unique across all virtual servers. Valid port numbers are 1 to 65535.

Defaults

No port number is defined.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

The Cisco BWG uses this port when sending delete notifications and NAI update messages to IOS SLB.

If multiple communication ports are needed, the network administrator must identify multiple unique unused ports.

Examples

The following example specifies that the Cisco BWG is to use port 63082 to communicate with IOS SLB:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# gw port 63082
```

Related Commands

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

hand-off radius

To change the amount of time IOS Server Load Balancing (IOS SLB) waits for an ACCT-START message from a new Mobile IP foreign agent in the event of a foreign agent hand-off, use the **hand-off radius** command in virtual server configuration mode. To restore the default hand-off timer, use the **no** form of this command.

hand-off radius *duration*

no hand-off radius

Syntax Description

duration	Hand-off timer duration in seconds. The valid range is 1 to 43200 seconds.

Defaults

No default behavior or values

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA2	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The hand-off radius timer is valid only for RADIUS virtual servers that have the **service radius** keywords specified on the **virtual** command.

Examples

The following example specifies that IOS SLB waits for 30 seconds after a foreign agent hand-off:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# hand-off radius 30
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

header

To configure the basic authentication values for the HTTP probe, use the **header** command in HTTP probe configuration mode. To remove a header HTTP probe configuration, use the **no** form of this command.

header *field-name* [*field-value*]

no header *field-name* [*field-value*]

Syntax Description

field-name	Configures the name of the HTTP probe header. The character string is limited to 15 characters.
field-value	(Optional) Configures the value of the HTTP probe header.

Defaults

The following headers are inserted in the request by default:

Accept: */*
Connection: close
User-Agent: cisco-slb-probe/1.0
Host: *virtual IP address*

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **header** command in HTTP probe configuration mode configures the name and value parameters of the header.

Note The colon (:) separating the field name and field value is automatically inserted if not provided. Multiple headers with the same name are not supported.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP configuration mode, and configures the HTTP probe header name as HeaderName and value as HeaderValue:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# header HeaderName HeaderValue
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

idle (firewall farm datagram protocol)

To specify the minimum time IOS Server Load Balancing (IOS SLB) maintains connection information in the absence of packet activity, use the **idle** command in firewall farm datagram protocol configuration mode. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle

Syntax Description

duration	Idle connection timer duration in seconds. Valid values range from 10 to 65535 seconds. The default is 3600 seconds (1 hour).

Defaults

The default idle duration is 3600 seconds.

Command Modes

Firewall farm datagram protocol configuration (config-slb-fw-udp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example instructs IOS SLB to maintain connection information for an idle connection for 120 seconds:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
Router(config-slb-fw-udp)# idle 120
```

Related Commands

Command	Description
protocol datagram	Enters firewall farm datagram protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.

idle (firewall farm TCP protocol)

To specify the minimum time IOS Server Load Balancing (IOS SLB) maintains connection information in the absence of packet activity, use the **idle** command in firewall farm TCP protocol configuration mode. To restore the default idle duration value, use the **no** form of this command.

idle *duration*

no idle

Syntax Description

duration	Idle connection timer duration in seconds. Valid values range from 10 to 65535 seconds. The default is 3600 seconds (1 hour).

Defaults

The default idle duration is 3600 seconds.

Command Modes

Firewall farm TCP protocol configuration (config-slb-fw-tcp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If a client sends a TCP packet that is not a sequence number (SYN) or reset (RST) packet, and IOS SLB does not have a TCP connection object in its table (possibly due to expiration of the idle timer), IOS SLB sends a TCP RST to the client.

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 IOS SLB.

Examples

The following example instructs IOS SLB to maintain connection information for an idle connection for 120 seconds:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# idle 120
```

Related Commands

Command	Description
protocol tcp	Enters firewall farm TCP protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.

idle (virtual server)

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

idle [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration* | **radius** {**request** | **framed-ip**} *duration*]

no idle [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration* | **radius** {**request** | **framed-ip**} *duration*]

Syntax Description

asn request	(Optional) For load balancing across a set of Access Service Network (ASN) gateways, configures the duration for which IOS SLB keeps the session object. If a Mobile Station (MS) Pre-Attachment Ack is received before the timer expires, IOS SLB resets the timer.
duration	Idle connection timer duration in seconds. Valid values range from 4 to 65535 seconds. For GTP IMSI, you can specify 0 to disable the timer and prevent GTP IMSI sticky database objects from timing out. The default values are: • 60 seconds in ASN load balancing. • 60 seconds for objects in the ASN MSID sticky database. • 0 seconds for objects in the GTP IMSI sticky database. • 10 seconds in the Home Agent Director. • 30 seconds in GPRS load balancing. • 30 seconds for RADIUS entries in the IOS SLB session database. • 7200 seconds for entries in the IOS SLB RADIUS framed-IP sticky database. • 3600 seconds (1 hour) in all other environments.
asn msid	(Optional) For load balancing across a set of ASN gateways, configures the duration for objects in the ASN Mobile Station ID (MSID) sticky database.
gtp imsi	(Optional) For general packet radio service (GPRS) Tunneling Protocol (GTP) cause code inspection, configures the duration for objects in the GTP International Mobile Subscriber ID (IMSI) sticky database.
query	(Optional) Query the Cisco gateway GPRS support node (GGSN) before deleting any GTP IMSI sticky objects. The default is not to query the GGSN.
max-queries	(Optional) Maximum number of queries to send when there is no response from the GGSN. Valid range is 1 to 10 queries. The default value is 5 queries.

gtp request	(Optional) For general packet radio service (GPRS) Tunneling Protocol (GTP) cause code inspection, configures the duration for Packet Data Protocol (PDP) context create, update, or delete request messages to a real gateway GPRS support node (GGSN) to go unanswered, before IOS SLB cleans up the session object.
ipmobile request	(Optional) For Home Agent Director, configures the duration for IOS SLB to wait for a Mobile IP Registration Request (RRQ), before IOS SLB cleans up the session object.
radius request	(Optional) Configures the duration for RADIUS entries in the IOS SLB session database.
radius framed-ip	(Optional) Configures the duration for entries in the IOS SLB RADIUS framed-IP sticky database.

Defaults

The default idle duration is:

- 60 seconds in ASN load balancing.
- 60 seconds for objects in the ASN MSID sticky database.
- 0 seconds for objects in the GTP IMSI sticky database.
- 10 seconds in the Home Agent Director
- 30 seconds in GPRS load balancing
- 30 seconds for RADIUS entries in the IOS SLB session database
- 7200 seconds for entries in the IOS SLB RADIUS framed-IP sticky database
- 3600 seconds (1 hour) in all other environments

The default setting for the **query** keyword is no queries.

The default setting for the *max-queries* argument is 5 queries.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(9)E	This command was modified to support GPRS load balancing.
12.1(11b)E	This command was modified to support RADIUS load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp request** keywords were added.
12.2(14)ZA2	The **ipmobile request** keywords were added.
12.2(18)SXE	The **gtp imsi** keywords were added.
12.2(18)SXF	The **query** keyword and *max-queries* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC1	The **asn request** option was added.

Release	Modification
12.2(33)SRE	The **asn msid** option was added.

Usage Guidelines

If a client sends a TCP packet that is not a sequence number (SYN) or reset (RST) packet, and IOS SLB does not have a TCP connection object in its table (possibly due to expiration of the idle timer), IOS SLB sends a TCP RST to the client.

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 (except in GPRS load balancing); such a low value can reduce the efficiency of the IOS SLB feature.

In most environments, the idle timer times out data paths. However, in GPRS load balancing, it times out the session context for signaling paths (not data paths).

In GPRS load balancing without GTP cause code inspection enabled, you must specify an idle timer greater than the longest possible interval between PDP context requests on the serving GPRS support node (SGSN). The longest interval can be expressed using the following algorithm:

Longest interval = T3 x 2(N3-2)

where T3 is the SGSN's T3-RESPONSE counter value and N3 is the SGSN's N3-REQUESTS counter value.

For example, if the T3-RESPONSE counter value is 3 and the N3-REQUESTS counter value is 6, then:

Longest interval = 3 x 2(6-2) = 3 x 2(4) = 3 x 16 = 48 seconds

Given those values, you must specify an idle timer of at least 49 seconds.

Examples

The following example instructs IOS SLB to maintain sticky objects in the GTP IMSI sticky database for 120 seconds:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# idle gtp imsi 120
```

Related Commands

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

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 (config-dfp)

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.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

- The DFP agent has been enabled using the **inservice (DFP agent)** command.
- The client subsystem has changed the DFP agent's state to **ACTIVE**.

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
agent	Identifies a DFP agent to which IOS SLB can connect.
ip dfp agent	Identifies a DFP agent subsystem and initiates DFP agent configuration mode.

Command	Description
ip slb dfp	Configures DFP, supplies an optional password, and initiates DFP configuration mode.

inservice (firewall farm)

To enable the firewall farm for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in firewall farm configuration mode. To remove the firewall farm 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 firewall farm for use with stateless and stateful backup.
group-name	(Optional) HSRP group name with which the IOS SLB firewall farm is associated.

Defaults

The firewall farm is defined to IOS SLB but is not used.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you use the **no** form of this command to remove a firewall farm from service, the firewall farm acquiesces gracefully. No new connections are assigned, and existing connections are allowed to complete.

Examples

In the following example, the firewall farm is enabled for use by the IOS SLB feature:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# inservice
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall by IP address farm and enters firewall farm configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.

inservice (firewall farm real server)

To enable the firewall for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in firewall farm real server configuration mode. To remove the firewall from service, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The firewall is defined to IOS SLB but is not used.

Command Modes

Firewall farm real server configuration (config-slb-fw-real)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

IOS SLB firewall load balancing uses probes to detect failures. Therefore, if you have not configured a probe, the firewall is not placed in service.

When you use the **no** form of this command to remove a firewall from service, the firewall acquiesces gracefully. No new connections are assigned, and existing connections are allowed to complete.

Examples

In the following example, the firewall is enabled for use by the IOS SLB feature:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# real 10.10.1.1
Router(config-slb-fw-real)# inservice
```

Related Commands

Command	Description
real (firewall farm)	Identifies a firewall by IP address as a member of a firewall farm and enters real server configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb reals	Displays information about the real servers.

inservice (server farm real server)

To enable the real server for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in SLB server farm real server configuration mode. 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

The real server is defined to IOS SLB but is not used.

Command Modes

SLB server farm real server configuration (config-slb-sfarm-real)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example, the real server is enabled for use by the IOS SLB feature:

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

Related Commands

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

inservice (server farm virtual server)

To enable the virtual server for use by IOS Server Load Balancing (IOS SLB), use the **inservice** command in SLB server farm virtual server configuration mode. To remove the virtual server from service, use the **no** form of this command.

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

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

Syntax Description

standby	(Optional) Configures the Hot Standby Router Protocol (HSRP) standby virtual server for use with stateless and stateful backup.
group-name	(Optional) HSRP group name with which the IOS SLB virtual server is associated.
active	(Optional) Enables the virtual server to stop answering Internet Control Message Protocol (ICMP) requests if all real servers associated with the virtual server are inactive.

Defaults

The virtual server is defined to IOS SLB but is not used.

Command Modes

SLB server farm virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(1)E	The **standby** keyword and *group-name* argument were added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **active** keyword was added.

Usage Guidelines

When you use the **no** form of this command to remove a virtual server from service, the virtual server acquiesces gracefully. No new connections are assigned, and existing connections are allowed to complete.

If the **active** keyword is configured, and all of the real servers that are associated with the virtual server are inactive, the following actions occur:

- The virtual server is placed in the INOP_REAL state.
- An SNMP trap is generated for the virtual server's state transition.
- The virtual server stops answering ICMP requests.

Examples

In the following example, the virtual server is enabled for use by the IOS SLB feature:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# inservice
```

Related Commands

Command	Description
show ip slb vservers	Displays information about the virtual servers.
virtual	Configures the virtual server attributes.

interval (custom UDP probe)

To configure a custom User Datagram Protocol (UDP) probe interval, use the **interval** command in custom UDP probe configuration mode. To remove a custom UDP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

seconds	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 10 seconds.

Defaults

The default custom UDP probe interval value is 10 seconds.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a custom UDP probe named PROBE6, enters custom UDP configuration mode, and configures the custom UDP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# interval 11
```

Related Commands

Command	Description
ip slb probe custom udp	Configures a custom User Datagram Protocol (UDP) probe name and enters custom UDP probe configuration mode.
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

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*

Syntax Description

seconds	Number of seconds to wait before recalculating weights for the DFP manager. The valid range is from 5 to 65535 seconds. The default is 10 seconds.

Defaults

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

Command Modes

DFP agent configuration (config-dfp)

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.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The DFP agent sends a 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
```

Related Commands

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

interval (DNS probe)

To configure a DNS probe interval, use the **interval** command in DNS probe configuration mode. To remove a DNS probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

seconds	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 10 seconds.

Defaults

The default DNS probe interval value is 10 seconds.

Command Modes

DNS probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a DNS probe named PROBE4, enters DNS configuration mode, and configures the DNS probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# interval 11
```

Related Commands

Command	Description
ip slb probe dns	Configures a DNS-probe name and enters DNS probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

interval (HTTP probe)

To configure an HTTP probe interval, use the **interval** command in HTTP probe configuration mode. To remove an HTTP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

seconds	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 8 seconds.

Defaults

The default HTTP probe interval value is 8 seconds.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP configuration mode, and configures the HTTP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# interval 11
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

interval (ping probe)

To configure a ping probe interval, use the **interval** command in ping probe configuration mode. To remove a ping probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

seconds	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 1 second.

Defaults

The default ping probe interval value is 1 second.

Command Modes

Ping probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a ping probe named PROBE1, enters ping configuration mode, and configures the ping probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE1 ping
Router(config-slb-probe)# interval 11
```

Related Commands

Command	Description
ip slb probe ping	Configures a ping probe name and enters ping probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

interval (TCP probe)

To configure a TCP probe interval, use the **interval** command in TCP probe configuration mode. To remove a TCP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

seconds	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 10 seconds.

Defaults

The default TCP probe interval value is 10 seconds.

Command Modes

TCP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a TCP probe named PROBE5, enters TCP configuration mode, and configures the TCP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE5 tcp
Router(config-slb-probe)# interval 11
```

Related Commands

Command	Description
ip slb probe tcp	Configures a TCP probe name and enters TCP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

interval (WSP probe)

To configure a Wireless Session Protocol (WSP) probe interval, use the **interval** command in WSP probe configuration mode. To remove a WSP probe interval configuration, use the **no** form of this command.

interval *seconds*

no interval *seconds*

Syntax Description

seconds	Number of seconds to wait before reattempting the probe. Valid values range from 1 to 65535 seconds. The default interval is 8 seconds.

Defaults

The default WSP probe interval value is 8 seconds.

Command Modes

WSP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(5a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a ping probe named PROBE3, enters WSP probe configuration mode, and configures the WSP probe timer interval to send every 11 seconds:

```
Router(config)# ip slb probe PROBE3 wsp
Router(config-slb-probe)# interval 11
```

Related Commands

Command	Description
ip slb probe wsp	Configures a WSP probe name and enters WSP probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

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 (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The **access-violations** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **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. If the **access-violations** keyword is specified and any IP access list is being used on an interface, then only process switching can generate accurate statistics (IP fast switching or CEF cannot).

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
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	Displays the active accounting or checkpointed database or displays access list violations.

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

ip-address	IP address in dotted decimal format.
wildcard	Wildcard bits to be applied to the *ip-address* argument.

Defaults

No filters are defined.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The *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
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.

Command	Description
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	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 Media Access Control (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

input	Performs accounting based on the source MAC address on received packets.
output	Performs accounting based on the destination MAC address on transmitted packets.

Defaults

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

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
```

Cisco uBR10012 Universal Broadband Router

The following example enables IP accounting based on the source MAC address for received packets on a Gigabit Ethernet interface:

```
Router#configure terminal
Router(config)#interface GigabitEthernet3/0/0
Router(config-if)#ip accounting mac-address input
```

Related Commands

Command	Description
show interface mac	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	Performs accounting based on IP precedence on received packets.
output	Performs accounting based on IP precedence on transmitted packets.

Command Default

IP accounting is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 Cisco Express Forwarding (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
show interface precedence	Displays precedence accounting information for an interface configured for precedence accounting.

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*

Syntax Description

threshold	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 (config)

Command History

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

Usage Guidelines

The 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
```

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.

Command	Description
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.
show ip accounting	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

Syntax Description

count	Number of transit records to store in the IP accounting database.

Defaults

The default number of transit records that are stored in the IP accounting database is 0.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Transit entries are those that do not match any of the filters specified by **ip accounting-list** global configuration commands. If no filters are defined, no transit entries are possible.

To maintain accurate accounting totals, the Cisco IOS software maintains two accounting databases: an active and a checkpointed database.

Examples

The following example specifies that no more than 100 transit records are stored:

```
ip accounting-transits 100
```

Related Commands

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

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*]

Syntax Description

ip-address	(Optional) IP broadcast address for a network.

Defaults

Default address: 255.255.255.255 (all ones)

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example specifies an IP broadcast address of 0.0.0.0:

```
ip broadcast-address 0.0.0.0
```

ip casa

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

ip casa *control-address igmp-address* [*udp-limit*]

no ip casa

Syntax Description

control-address	IP address of the forwarding agent side of the services manager and forwarding agent tunnel used for sending signals. This address is unique for each forwarding agent.
igmp-address	Interior Gateway Management Protocol (IGMP) address on which the forwarding agent will listen for wildcard and fixed affinities.
udp-limit	(Optional) Maximum User Datagram Protocol (UDP) queue length; valid values are from 50 to 65535. The default is 256.

Defaults

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(17d)SXB1	Support for this command was added for Catalyst 6500 series switches.
12.2(18)SXF6	The *udp-limit* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If more than the maximum *udp-limit* value arrives in a burst, the Cisco Appliance Services Architecture (CASA) wildcard updates from the service manager might get dropped.

The *control-address* value is unique for each forwarding agent.

Examples

The following example specifies the Internet address (10.10.4.1) and IGMP address (224.0.1.2) for the forwarding agent and sets the UDP queue length to 300:

```
ip casa 10.10.4.1 224.0.1.2 300
```

Related Commands

Command	Description
forwarding-agent	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) sets up or tears down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** command in global configuration mode. 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

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

Defaults

Load interval: 30 seconds
Update rate: 10 seconds

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **ip nhrp trigger-svc** command sets the threshold by which NHRP sets up and tears down a connection. The threshold is the Cisco Express Forwarding 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 Cisco Express Forwarding 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
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

ip dfp agent

To identify a Dynamic Feedback Protocol (DFP) agent subsystem and enter 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*

Syntax Description

subsystem-name	Character string used to identify the DFP agent subsystem: • **slb** for IOS SLB • **mobileip** for Mobile IP and the Home Agent Director The subsystem name enables the subsystem to send weights to a DFP manager. The subsystem name is limited to 15 characters.

Defaults

No DFP agent subsystem is defined.

Command Modes

Global configuration (config)

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.
12.2(18)SXD	The **mobileip** subsystem name was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To discover the subsystem names that are available in your network, enter the **ip dfp agent ?** command.

Examples

The following example identifies a DFP agent subsystem named **slb**:

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

Related Commands

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

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

access-list-number	(Optional) Standard access list number in the range from 1 to 199. If specified, a broadcast must pass the access list to be forwarded.
extended access-list-number	(Optional) Extended access list number in the range from 1300 to 2699.

Defaults

Disabled; all IP directed broadcasts are dropped.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The default behavior changed to directed broadcasts being dropped.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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** 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
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

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

udp	Forwards User Datagram Protocol (UDP) packets. See the "Usage Guidelines" section for a list of port numbers forwarded by default.
port	(Optional) Destination port that controls which UDP services are forwarded.
nd	Forwards Network Disk (ND) packets. This protocol is used by older diskless Sun workstations.
sdns	Secure Data Network Service.

Defaults

Enabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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 packets (ports 67 and 68)
- TACACS service (port 49)
- IEN-116 Name Service (port 42)



Note If UDP port 68 is used as the destination port number, it is not forwarded by default.

Examples

The following example defines a helper address and uses the **ip forward-protocol** command. Using the **udp** keyword without specifying any port numbers will allow forwarding of UDP packets on the default ports.

```
ip forward-protocol udp
interface ethernet 1
 ip helper-address 10.24.42.2
```

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**]

Syntax Description

any-local-broadcast	(Optional) Accept any local broadcast when flooding.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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 **no 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 User Datagram Protocol (UDP) (17).
- The UDP destination port must be TFTP, Domain Name System (DNS), Time, NetBIOS, ND, or BOOTP packet, or a UDP port specified by the **ip forward-protocol udp** command.

A flooded UDP datagram is given the destination address specified by the **ip broadcast-address** 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 *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 (10.108.255.255 as an example in the network number 10.108.0.0). This mechanism also forward packets whose contents are the zeros version of the all-networks broadcast when subnetting is enabled (for example, 10.108.0.0).

This command is an extension of the **ip helper-address** 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
ip broadcast-address	Defines a broadcast address for an interface.
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.
ip forward-protocol turbo-flood	Speeds up flooding of UDP datagrams using the spanning-tree algorithm.
ip helper-address	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 [**udp-checksum**]

no ip forward-protocol turbo-flood [**udp-checksum**]

Syntax Description

udp-checksum	(Optional) UDP checksum.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(17d)SXB7	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Used in conjunction with the **ip forward-protocol spanning-tree** command, this command 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.

When you enter the **ip forward-protocol turbo-flood** command, the outgoing UDP packets have a NULL checksum. If you want to have UDP checksums on all outgoing packets, you must enter the **ip forward-protocol turbo-flood udp-checksum** command.

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 10.9.1.1
 bridge-group 1
!
interface ethernet 1
 ip address 10.9.1.2
 bridge-group 1
!
 bridge 1 protocol dec
```

The following example shows how to speed up the flooding of UDP packets using the spanning-tree algorithm and include the UDP checksums on all outgoing packets:

```
ip forward-protocol turbo-flood udp-checksum
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports are forwarded by the router when forwarding broadcast packets.
ip forward-protocol spanning-tree	Permits IP broadcasts to be flooded throughout the internetwork in a controlled fashion.

ip header-compression special-vj

To enable the special Van Jacobson (VJ) format of TCP header compression, use the **ip header-compression special-vj** command in interface configuration mode. To disable the special VJ format and return to the default VJ format, use the **no** form of this command.

ip header-compression special-vj

no ip header-compression special-vj

Syntax Description

This command has no arguments or keywords.

Command Default

The default VJ format of TCP header compression is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)T12	This command was introduced.
15.0(1)M2	This command was integrated into Cisco IOS Release 15.0(1)M2.

Usage Guidelines

Use the **ip tcp header-compression** command to enable the default VJ format of TCP header compression. Then use the **ip header-compression special-vj** command to enable the special VJ format of TCP header compression.

To enable the special VJ format of TCP header compression so that context IDs are included in compressed packets, use the **special-vj** command in IPHC profile configuration mode.

Examples

The following example shows how to configure the special VJ format of TCP header compression for serial interface 5/0:

```
Router(config)# interface serial 5/0
Router(config-if)# ip header-compression special-vj

Building configuration...

Current configuration : 579 bytes
!
interface Serial 5/0
 bandwidth 4032
 ip address 10.72.72.3 255.255.255.0
 encapsulation frame-relay
 shutdown
 no keepalive
 serial restart-delay 0
 no arp frame-relay
 frame-relay map ip 10.72.72.2 100 broadcast
 frame-relay ip tcp header-compression
```

```
 frame-relay ip tcp compression-connections 8
 frame-relay ip rtp header-compression periodic-refresh
 frame-relay ip rtp compression-connections 8
 service-policy output p1
 ip header-compression special-vj
 ip header-compression max-header 60
 ip header-compression max-time 50
 ip header-compression max-period 32786
end
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.
show ip tcp header-compression	Displays TCP/IP header compression statistics.
special-vj	Enables the special VJ format of TCP header compression so that context IDs are included in compressed packets.

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

vrf *name*	(Optional) Enables VPN routing and forwarding (VRF) instance and VRF name.
global	(Optional) Configures a global routing table.
address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.
redundancy *vrg-name*	(Optional) Defines the VRG group name.

Defaults

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)B	The **vrf** *name* keyword and argument combination was added, and the **global** keyword was added.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(15)T	The **redundancy** *vrg-name* keyword and argument combination was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Combined with the **ip forward-protocol** 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** command in global configuration mode.

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 10.24.43.2
```

The following example defines an address that acts as a helper address and is associated with the VRF named host1:

```
interface ethernet 1/0
 ip helper-address vrf host1 10.25.44.2
```

The following example defines an address that acts as a helper address and is associated with the VRG named group1:

```
interface ethernet 1/0
 ip helper-address 10.25.45.2 redundancy group1
```

Related Commands

Command	Description
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip icmp rate-limit unreachable

To limit the rate at which Internet Control Message Protocol (ICMP) unreachable messages are generated for a destination, use the **ip icmp rate-limit unreachable** command in global configuration mode. To use the default, use the **no** form of this command.

ip icmp rate-limit unreachable [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]

no ip icmp rate-limit unreachable [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]

Syntax Description

df	(Optional) Don't Fragment (DF) bit is set. The optional *ms* argument is a time limit in milliseconds (ms) in which one unreachable message is generated. If the **df** keyword is specified, its *ms* argument remains independent from those of general destination unreachable messages. The valid range is from 1 ms to 4294967295 ms. **Note** Counting begins as soon as this command is configured.
log	(Optional) Logging of generated messages that show packets that could not reach a destination at a specified threshold. The optional *packets* argument specifies a packet threshold. When it is reached, a log message is generated on the console. The default is 1000 packets. The optional *interval-ms* argument is a time limit for the interval for which a logging message is triggered. The default is 60000 ms, which is 1 minute.

Defaults

The default value is one ICMP destination unreachable message per 500 ms.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced.
12.4(2)T	The *packets* and the *interval-ms* arguments and **log** keyword were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Counting of packets begins when the command is configured and a packet threshold is specified.

The **no ip icmp rate-limit unreachable** command turns off the previously configured rate limit. To reset the rate limit to its default value, use the **ip icmp rate-limit unreachable** command default.

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 in ms for DF destination unreachable messages.

Examples

The following example sets the rate of the ICMP destination unreachable message to one message every 10 ms:

```
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:

```
no ip icmp rate-limit unreachable
```

The following example sets a logging packet threshold and time interval:

```
ip icmp rate-limit unreachable log 1200 120000
```

Related Commands

Command	Description
clear ip icmp rate-limit	Clears all ICMP unreachable destination messages or all statistics for a specified interface.
show ip icmp rate-limit	Displays all ICMP unreachable destination messages or all statistics for a specified interface.

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

host	(Optional) Sends ICMP host redirects.
subnet	(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 (config)

Command History

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

Usage Guidelines

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 host
```

The following example sets the value back to the default, which is subnet redirects:

```
ip icmp redirect subnet
```

Related Commands

Command	Description
ip redirects	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 ip information-reply

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The 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 10.108.1.0 255.255.255.0
 ip information-reply
```

ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** command in interface configuration mode. 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

multicast	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.
holdtime *seconds*	(Optional) Length of time in seconds that advertisements are held valid. Default is three times the **maxadvertinterval** value. Must be greater than **maxadvertinterval** and cannot be greater than 9000 seconds.
maxadvertinterval *seconds*	(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.
minadvertinterval *seconds*	(Optional) Minimum interval in seconds between advertisements. The range is from 1 to 1800. The default is 450 seconds.
preference *number*	(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.
address *address* [*number*]	(Optional) IP address (*address*) to proxy advertise, and optionally, its preference value (*number*).

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 (config-if)

Command History

Release	Modification
10.0	This command was introduced.

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

Usage Guidelines

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 0 to 900.

 ip irdp preference 900

!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 10.108.14.5 with default router preference.

 ip irdp address 10.108.14.5

!Proxy-advertise 10.108.14.6 with preference of 50.

 ip irdp address 10.108.14.6 50
```

Related Commands

Command	Description
show ip irdp	Displays IRDP values.

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 (config-if)

Command History

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

Examples

The following example enables the sending of ICMP mask reply messages on Ethernet interface 0:

```
interface ethernet 0
 ip address 10.108.1.0 255.255.255.0
 ip mask-reply
```

ip mtu

To set the maximum transmission unit (MTU) size of IP packets that are 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

Syntax Description

bytes	MTU, in bytes.

Command Default

The IP MTU default value depends on the interface medium. Table 1 lists default MTU values according to media type.

Table 1 Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470
VASI	9216

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

If an IP packet exceeds the MTU that is set for the interface, the Cisco IOS software will fragment it.

For VASI interfaces that involve Ethernet type interfaces (Ethernet, Fast Ethernet or Gigabit Ethernet), the IP MTU of the VASI interface must be set the same as the lower default setting of the Ethernet type interface of 1500 bytes. If this adjustment is not made, OSPF reconvergence on the VASI interface will take too long.

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.

Examples

The following example sets the maximum IP packet size for the first serial interface to 300 bytes:

```
Router(config)# interface serial 0
Router(config-if)# ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the maximum packet size or MTU size.

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 (config-if)

Command History

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

Usage Guidelines

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
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip sctp asconf

To enable the ability of an existing Stream Control Transmission Protocol (SCTP) endpoint to automatically send Address Configuration Change (ASCONF) chunks in response to an IP address change on a router without an authentication check, use the **ip sctp asconf** command in global configuration mode. To disable the requirement for ASCONF and ASCONF Acknowledgement (ASCONF-ACK) chunks to perform an authentication requirement check, use the **no** form of this command.

ip sctp asconf {**authenticate check** | **auto**}

no ip sctp asconf {**authenticate check** | **auto**}

Syntax Description

authenticate check	Configures SCTP to check that authentication is supported on the endpoint before sending an ASCONF chunk.
auto	Configures SCTP to automatically send ASCONF chunks in response to an IP address change on a router.

Command Default

SCTP checks the authentication status of the endpoint before sending an ASCONF chunk in response to an IP address change on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The ASCONF chunk format requires the receiving SCTP to not report to the sender if it does not understand the ASCONF chunk. This command enables you to configure sending the ASCONF chunk automatically in response to an IP address change in an SCTP stream, or to authenticate the endpoint before sending the ASCONF chunk.

The ASCONF chunk is used to communicate to the endpoint of an SCTP stream that at least one of the configuration change requests in the stream must be acknowledged.

Examples

The following example shows how to configure SCTP to authenticate the endpoint before sending an ASCONF chunk:

```
Router(config)# ip sctp asconf authenticate check
```

The following example shows how to configure SCTP to automatically send an ASCONF chunk in response to a change in the IP address of the remote endpoint:

```
Router(config)# ip sctp asconf auto
```

Related Commands

Command	Description
ip sctp authenticate	To define Stream Control Transmission Protocol (SCTP) data chunks that the client requires be authenticated.

ip sctp authenticate

To define Stream Control Transmission Protocol (SCTP) data chunks that the client requires be authenticated, use the **ip sctp authenticate** command in global configuration mode. To disable the authentication of an SCTP data chunk, use the **no** form of this command.

ip sctp authenticate {*chunk-type* | *chunk-number*}

no ip sctp authenticate {*chunk-type* | *chunk-number*}

Syntax Description

chunk-type	Name of the chunk type to be authenticated. See Table 1 in the "Usage Guidelines" section for a list of chunk types.
chunk-number	Number of the chunk to be authenticated in the range from 0 to 255.

Command Default

SCTP data chunks are not authenticated by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	This command was enhanced to support the Address Configuration (ASCONF) and ASCONF-ACK SCTP chunk types.

Usage Guidelines

SCTP Authentication procedures use either Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1), which can be memory and CPU intensive. Enabling SCTP Authentication on data chunks could impact CPU utilization when a large number of authenticated chunks are sent.

You cannot disable the authentication of the ASCONF or ASCONF-ACK chunks.

Enabling the authentication of a chunk type applies only to new endpoints and associations.

Table 2 provides a list of SCTP chunk types and SCTP chunk numbers.

Table 2 SCTP Authentication Chunk Types

SCTP Chunk Type	SCTP Chunk Number	Description
abort association	0x06	ABORT chunk.
asconf	0xC1	ASCONF chunk.
asconf-ack	0x80	ASCONF acknowledgement chunk.
cookie-ack	0x0b	COOKIE acknowledgment chunk.
cookie-echo	0x0a	COOKIE-ECHO chunk.
data	0x00	DATA chunk.

Table 2 SCTP Authentication Chunk Types

SCTP Chunk Type	SCTP Chunk Number	Description
fwd-tsn	0xc0	FWD-CUM-TSN chunk. Forwarded cumulative transmission sequence number chunk.
heartbeat	0x04	HEARTBEAT request chunk.
heartbeat-ack	0x05	HEARTBEAT acknowledgement chunk.
packet-drop	0x81	PACKET-DROP chunk.
sack	0x03	Selective acknowledgment chunk.
shutdown	0x07	SHUTDOWN chunk.
shutdown-ack	0x08	SHUTDOWN acknowledgment chunk.
stream-reset	0x82	STREAM-RESET chunk.

Examples

The following example shows how to enable authentication of SCTP data chunks:

```
ip sctp authenticate data
```

Related Commands

Command	Description
show sctp association	Displays accumulated information for a specific SCTP association.
show sctp errors	Displays the error counts logged by SCTP.
show sctp statistics	Displays the overall statistics counts for SCTP activity.

ip slb capp udp

To enable the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enter SLB Content Application Peering Protocol (CAPP) configuration mode, use the **ip slb capp udp** command in global configuration mode. To disable the KAL-AP agent feature, use the **no** form of this command.

ip slb capp udp

no ip slb capp udp

Syntax Description

This command has no arguments or keywords.

Defaults

The KAL-AP agent is not enabled.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example enables the KAL-AP agent an enters CAPP UDP configuration mode:

```
Router(config)# ip slb capp udp
```

Related Commands

Command	Description
farm-weight	Specifies a weight to be used by the IOS SLB KeepAlive Application Protocol (KAL-AP) agent when calculating the load value for a server farm.
kal-ap domain	Specifies a domain tag to be used by the IOS SLB KeepAlive Application Protocol (KAL-AP) agent when searching for a server farm.
peer port	Specifies the port to which the IOS SLB KeepAlive Application Protocol (KAL-AP) agent is to connect.
peer secret	Enables Message Digest Algorithm Version 5 (MD5) authentication for the IOS SLB KeepAlive Application Protocol (KAL-AP) agent.

ip slb dfp

To configure Dynamic Feedback Protocol (DFP), supply an optional password, and enter DFP configuration mode, 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** [*encrypt*] *secret-string* [*timeout*]]

no ip slb dfp

Syntax Description

password	(Optional) Password for Message Digest Algorithm Version 5 (MD5) authentication.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
timeout	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted. The valid range is 0 to 65535 seconds. The default value is 180 seconds, if a password is specified.

Defaults

The default password encryption is 0 (unencrypted).
The default password timeout is 180 seconds, if a password is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.

Release	Modification
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(3a)E	The **0** and **7** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The password specified in the **ip slb dfp** command for the DFP manager must match the password specified in the **password** command for the DFP 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 to allow enough time for you to update the password on all agents and servers before the timeout expires. Setting a longer timeout 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.

If you are running IOS SLB as a DFP manager, and you specify a password on the **ip slb dfp** command, the password must match the one specified on the **password** command in DFP agent configuration mode in the DFP agent.

Examples

The following example configures DFP, sets the DFP password to Password1 and the timeout to 360 seconds, and enters DFP configuration mode:

```
Router(config)# ip slb dfp password Password1 360
Router(config-slb-dfp)#
```

Related Commands

Command	Description
agent	Identifies a DFP agent to which IOS SLB can connect.
ip dfp agent	Identifies a DFP agent subsystem and enters DFP agent configuration mode.

ip slb entries

To configure an initial allocation and a maximum value for IOS Server Load Balancing (IOS SLB) database entries, use the **ip slb entries** command in global configuration mode. To restore the default values, use the **no** form of this command.

ip slb entries [**conn** [*init-conn* [*max-conn*]] | **frag** [*init-frag* [*max-frag*] | **lifetime** *timeout*] | **gtp** {**gsn** *init-gsn* [*max-gsn*] | **nsapi** *init-nsapi* [*max-nsapi*]} | **sticky** [*init-sticky* [*max-sticky*]]]

no ip slb entries [**conn** | **frag** [**lifetime**] | **gtp** {**gsn** | **nsapi**} | **sticky**]

Syntax Description

conn	(Optional) Configures an initial allocation and a maximum value for IOS SLB connection database entries.
init-conn	(Optional) Initial allocation of connection database entries. When the number of available entries is reduced to less than half of the *init-conn* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-conn* argument. Valid range is 1 to 1000000 connection database entries. The default is 8000 connection database entries. **Note** Be careful when setting the *init-conn* argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
max-conn	(Optional) Maximum number of connection database entries that can be allocated. Valid range is 1 to 8000000 connection database entries. The default is 8000000 connection database entries.
frag	(Optional) Configures an initial allocation and a maximum value for IOS SLB fragment database entries.
init-frag	(Optional) Initial allocation of routing entries in the fragment database. When the number of available entries is reduced to less than half of the *init-frag* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-frag* argument. Valid range is 1 to 1000000 connection database entries. The default is 2000 connection database entries. **Note** Be careful when setting the *init-frag* argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
max-frag	(Optional) Maximum number of fragment database entries that can be allocated. Valid range is 1 to 8000000 fragment database entries. The default is 32000 fragment database entries.

lifetime *timeout*	(Optional) Lifetime of an entry in the IOS SLB fragment database, in seconds. Valid range is 1 to 255 seconds. The default value is 10 seconds.
gtp	(Optional) Configures an initial allocation and a maximum value for IOS SLB general packet radio service (GPRS) Tunneling Protocol (GTP) database entries.
gsn	(Optional) Configures an initial allocation and a maximum value for IOS SLB GPRS support node (GSN) database entries.
init-gsn	(Optional) Initial allocation of GSN database entries. When the number of available entries is reduced to less than half of the *init-gsn* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-gsn* argument. Valid range is 1 to 5000 GSN database entries. The default is 200 GSN database entries. **Note** Be careful when setting the *init-gsn* argument to a very high value, such as 5000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 500.
max-gsn	(Optional) Maximum number of GSN database entries that can be allocated. Valid range is 1 to 20000 GSN database entries. The default is 20000 GSN database entries.
nsapi	(Optional) Configures an initial allocation and a maximum value for IOS SLB Network Service Access Point Identifier (NSAPI) database entries.
init-nsapi	(Optional) Initial allocation of NSAPI database entries. When the number of available entries is reduced to less than half of the *init-nsapi* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-nsapi* argument. Valid range is 1 to 1000000 NSAPI database entries. The default is 8000 NSAPI database entries. **Note** Be careful when setting the *init-nsapi* argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
max-nsapi	(Optional) Maximum number of NSAPI database entries that can be allocated. Valid range is 1 to 8000000 NSAPI database entries. The default is 8000000 NSAPI database entries.
sticky	(Optional) Configures an initial allocation and a maximum value for IOS SLB sticky connection database entries.

lifetime *timeout*	(Optional) Lifetime of an entry in the IOS SLB fragment database, in seconds. Valid range is 1 to 255 seconds. The default value is 10 seconds.
gtp	(Optional) Configures an initial allocation and a maximum value for IOS SLB general packet radio service (GPRS) Tunneling Protocol (GTP) database entries.
gsn	(Optional) Configures an initial allocation and a maximum value for IOS SLB GPRS support node (GSN) database entries.
init-gsn	(Optional) Initial allocation of GSN database entries. When the number of available entries is reduced to less than half of the *init-gsn* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-gsn* argument. Valid range is 1 to 5000 GSN database entries. The default is 200 GSN database entries. **Note** Be careful when setting the *init-gsn* argument to a very high value, such as 5000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 500.
max-gsn	(Optional) Maximum number of GSN database entries that can be allocated. Valid range is 1 to 20000 GSN database entries. The default is 20000 GSN database entries.
nsapi	(Optional) Configures an initial allocation and a maximum value for IOS SLB Network Service Access Point Identifier (NSAPI) database entries.
init-nsapi	(Optional) Initial allocation of NSAPI database entries. When the number of available entries is reduced to less than half of the *init-nsapi* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-nsapi* argument. Valid range is 1 to 1000000 NSAPI database entries. The default is 8000 NSAPI database entries. **Note** Be careful when setting the *init-nsapi* argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
max-nsapi	(Optional) Maximum number of NSAPI database entries that can be allocated. Valid range is 1 to 8000000 NSAPI database entries. The default is 8000000 NSAPI database entries.
sticky	(Optional) Configures an initial allocation and a maximum value for IOS SLB sticky connection database entries.

init-sticky	(Optional) Initial allocation of sticky database entries. When the number of available entries is reduced to less than half of the *init-sticky* argument, IOS SLB begins allocating additional entries. The number of entries can grow dynamically up to the number specified by the *max-sticky* argument. Valid range is 1 to 1000000 sticky database entries. The default is 4000 sticky database entries. **Note** Be careful when setting the *init-sticky* argument to a very high value, such as 1000000, because IOS SLB immediately allocates those entries, which can cause the router or switch to pause indefinitely. Start with a lower value, such as 125000.
max-sticky	(Optional) Maximum number of sticky database entries that can be allocated. Valid range is 1 to 8000000 sticky database entries. The default is 8000000 sticky database entries.

Defaults

For the connection database, the default initial allocation is 8000 connections, and the default maximum is 8000000 connections.
For the fragment database, the default initial allocation is 2000 fragments, and the default maximum is 8000000 fragments. The default lifetime is 10 seconds.
For the GSN database, the default initial allocation is 200 GSNs, and the default maximum is 20000 GSNs.
For the NSAPI database, the default initial allocation is 8000 NSAPIs, and the default maximum is 8000000 NSAPIs.
For the sticky connection database, the default initial allocation is 4000 sticky connections, and the default maximum is 3200 sticky connections.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(11b)E	The **lifetime** keyword and *timeout* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gsn**, **gtp**, and **nsapi** keywords and *init-gsn*, *init-nsapi*, *max-gsn*, and *max-nsapi* arguments were added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enter this command *before* entering the rest of your IOS SLB configuration. If you have already begun configuring IOS SLB before entering this command, you must reload ISO SLB after entering this command.

If you configure an initial allocation value that exceeds the amount of available memory, memory might not be available for other features. In extreme cases, the router or switch might not boot properly. Therefore, be careful when you configure initial allocation values.

Examples

The following example configures an initial allocation of 128,000 connections, which can grow dynamically to a limit of 512,000 connections:

```
Router(config)# ip slb entries conn 128000 512000
```

Related Commands

Command	Description
show ip slb conns	Displays all connections handled by IOS SLB, or, optionally, only those connections associated with a particular virtual server or client.

ip slb firewallfarm

To identify a firewall farm and enter firewall farm configuration mode, use the **ip slb firewallfarm** command in global configuration mode. To remove the firewall farm from the IOS Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

ip slb firewallfarm *firewall-farm*

no ip slb firewallfarm *firewall-farm*

Syntax Description

firewall-farm	Character string used to identify the firewall farm. The character string is limited to 15 characters.

Defaults

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Grouping real servers into firewall farms is an essential part of IOS SLB firewall load balancing. Using firewall farms enables IOS SLB to assign new connections to the real servers based on their weighted capacities, and on the load-balancing algorithms used.

Examples

The following example identifies a firewall farm named FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
```

Related Commands

Command	Description
real (firewall farm)	Identifies a firewall by IP address as a member of a firewall farm and enters real server configuration mode.

ip slb map

To configure an IOS SLB protocol map and enter SLB map configuration mode, use the **ip slb map** command in global configuration mode. To delete the map, use the **no** form of this command.

ip slb map *map-id* {**gtp** | **radius**}

no ip slb map *map-id* {**gtp** | **radius**}

Syntax Description

map-id	IOS SLB protocol map identifier. The valid range is from 1 to 255.
gtp	For general packet radio service (GPRS) load balancing, configures an IOS SLB GPRS Tunneling Protocol (GTP) map and enters SLB GTP map configuration mode.
radius	For RADIUS load balancing, configures an IOS SLB RADIUS map and enters SLB RADIUS map configuration mode.

Defaults

None

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You can configure up to 255 IOS SLB GTP or RADIUS maps. However, we recommend that you configure no more than 10 maps for a given virtual server.

Each map ID must be unique across all server farms associated with a given GTP or RADIUS virtual server. That is, you cannot configure more than one map with the same ID.

For each IOS SLB RADIUS map, you can configure a single **calling-station-id** command or a single **username (IOS SLB)** command, but not both.

Configure the **gtp** or **radius** keyword only on maps that are to be used with GTP or RADIUS virtual servers, respectively.

Examples

The following example configures IOS SLB RADIUS map **1** and enters SLB RADIUS map configuration mode:

```
Router(config)# ip slb map 1 radius
```

Related Commands

Command	Description
calling-station-id	Configures an ASCII regular expression string to be matched against the calling station ID attribute in the RADIUS payload.
show ip slb map	Displays information about IOS SLB protocol maps.
username (IOS SLB)	Configures an ASCII regular expression string to be matched against the username attribute in the RADIUS payload.

ip slb maxbuffers frag

To configure the maximum number of buffers for the IOS Server Load Balancing (IOS SLB) fragment database, use the **ip slb maxbuffers frag** command in global configuration mode. To restore the default setting, use the **no** form of this command.

ip slb maxbuffers frag *buffers*

no ip slb maxbuffers frag

Syntax Description

buffers	Maximum number of out-of-order trailing fragments to be buffered simultaneously in the IOS SLB fragment database, waiting for the leader fragment. This value can help prevent IOS SLB memory from being overrun in the event of a fragment attack. Valid range is 0 to 65535 buffers. The default value is 100 buffers.

Defaults

The default maximum is 100 buffers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example sets the maximum number of buffers for the IOS SLB fragment buffer to 300:

```
Router(config)# ip slb maxbuffers frag 300
```

ip slb natpool

To configure an IOS Server Load Balancing (IOS SLB) Network Address Translation (NAT) to create at least one client address pool, use the **ip slb natpool** command in global configuration mode. To remove an **ip slb natpool** configuration, use the **no** form of this command.

ip slb natpool *pool start-ip end-ip* [**netmask** *netmask* | **prefix-length** *leading-1-bits*] [**entries** *init-address* [*max-address*]]

no ip slb natpool *pool*

Syntax Description

pool	Character string used to identify this client address pool. The character string is limited to 15 characters.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask *netmask*	(Optional) Configures the mask for the associated IP subnet. Specifies the netmask of the network to which the pool addresses belong.
prefix-length *leading-1-bits*	(Optional) Specifies how many bits of the netmask are ones (that is, how many bits of the address indicate the network).
entries	(Optional) Configures an initial allocation and optional maximum value for IOS SLB client NAT address entries for the *pool* argument.
init-address	(Optional) Initial allocation of client NAT address entries. The number of client NAT address entries can grow dynamically: When the number of available client NAT address entries is less than half of the *init-address* argument, IOS SLB allocates additional client NAT address entries. Valid range is 1 to 1000000 client NAT address entries. The default is 8000 client NAT address entries.
max-address	(Optional) Maximum number of client NAT address entries that can be allocated. Valid range is 1 to 8000000 client NAT address entries. The default is the maximum number of ports that can be allocated within the IP address range specified for *pool*. For example, the following command: **ip slb natpool 10.1.10.1 10.1.10.5 prefix-length 24 entries 8000** has a default *max-address* of (10.1.10.1-10.1.10.1.5*54535, or 4*54535, or 218140.

Defaults

The default initial allocation is 8000 client NAT address entries.
The default maximum number of client NAT address entries that can be allocated is the maximum number of ports that can be allocated within the IP address range.

Command Modes Global configuration (config)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines If you want to use client NAT, you must create at least one client address pool.

The range of IP addresses in the address pool, configured with the *start-ip* and *end-ip* arguments, must not overlap the IP address for a VLAN as specified on the **ip address** interface configuration command.

Examples The following example configures an IOS SLB NAT server farm pool of addresses with the name web-clients, the IP address range from 10.1.10.1 to 10.1.10.5, and a subnet mask of 255.255.0.0:

```
Router(config)# ip slb natpool web-clients 10.1.10.1 10.1.10.5 netmask 255.255.0.0
```

Related Commands

Command	Description
show ip slb natpool	Displays information about the IOS SLB NAT configuration.
show ip slb serverfarms	Displays information about the server farm configuration.

ip slb probe custom udp

To configure a custom User Datagram Protocol (UDP) probe name and enter custom UDP probe configuration mode, use the **ip slb probe custom udp** command in global configuration mode. To remove a custom UDP probe name, use the **no** form of this command.

ip slb probe *probe* **custom udp**

no ip slb probe *probe*

Syntax Description

probe	Name of the custom UDP probe. The character string is limited to 15 characters.

Defaults

No custom UDP probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the custom UDP probe name and application protocol and enters custom UDP configuration mode.

The custom UDP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE6, then enters custom UDP probe configuration mode:

```
Router(config)# ip slb probe PROBE6 custom udp
```

Related Commands

Command	Description
address (custom UDP probe)	Configures an IP address to which to send custom UDP probes.
interval (custom UDP probe)	Configures a custom UDP probe interval.
port (custom UDP probe)	Specifies the port to which a custom UDP probe is to connect.
request (custom UDP probe)	Defines the payload of the UDP request packet to be sent by a custom UDP probe.
response	Defines the data string to match against custom UDP probe response packets.
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe dns

To configure a Domain Name System (DNS) probe name and enter DNS probe configuration mode, use the **ip slb probe dns** command in global configuration mode. To remove a DNS probe name, use the **no** form of this command.

ip slb probe *probe* **dns**

no ip slb probe *probe*

Syntax Description

probe	Name of the DNS probe. The character string is limited to 15 characters.

Defaults

No DNS probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

DNS probes send domain name resolve requests to real servers and verify the returned IP addresses.

This command configures the DNS probe name and application protocol and enters DNS configuration mode.

The DNS probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE4, then enters DNS probe configuration mode:

```
Router(config)# ip slb probe PROBE4 dns
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe http

To configure an HTTP probe name and enter HTTP probe configuration mode, use the **ip slb probe http** command in global configuration mode. To remove an HTTP probe name, use the **no** form of this command.

ip slb probe *probe* **http**

no ip slb probe *probe*

Syntax Description

probe	Name of the HTTP probe. The character string is limited to 15 characters.

Defaults

No HTTP probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the HTTP probe name and application protocol and enters HTTP configuration mode.

The HTTP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Note HTTP probes require a route to the virtual server. The route is not used, but it must exist to enable the sockets code to verify that the destination can be reached, which in turn is essential for HTTP probes to function correctly. The route can be either a host route (advertised by the virtual server) or a default route (specified using the **ip route 0.0.0.0 0.0.0.0** command, for example).

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE2, then enters HTTP probe configuration mode:

```
Router(config)# ip slb probe PROBE2 http
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe ping

To configure a ping probe name and enter ping probe configuration mode, use the **ip slb probe ping** command in global configuration mode. To remove a ping probe name, use the **no** form of this command.

ip slb probe *probe* **ping**

no ip slb probe *probe*

Syntax Description

probe	Name of the ping probe. The character string is limited to 15 characters.

Defaults

No ping probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the ping probe name and application protocol and enters ping configuration mode.

The ping probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE1, then enters ping probe configuration mode:

```
Router(config)# ip slb probe PROBE1 ping
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe tcp

To configure a TCP probe name and enter TCP probe configuration mode, use the **ip slb probe tcp** command in global configuration mode. To remove a TCP probe name, use the **no** form of this command.

ip slb probe *probe* **tcp**

no ip slb probe *probe*

Syntax Description

probe	Name of the TCP probe. The character string is limited to 15 characters.

Defaults

No TCP probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the TCP probe name and application protocol and enters TCP configuration mode.

The TCP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE5, then enters TCP probe configuration mode:

```
Router(config)# ip slb probe PROBE5 tcp
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb probe wsp

To configure a Wireless Session Protocol (WSP) probe name and enter WSP probe configuration mode, use the **ip slb probe wsp** command in global configuration mode. To remove a WSP probe name, use the **no** form of this command.

ip slb probe *probe* **wsp**

no ip slb probe *probe*

Syntax Description

probe	Name of the WSP probe. The character string is limited to 15 characters.

Defaults

No WSP probe is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the WSP probe name and application protocol and enters WSP probe configuration mode.

The WSP probe cannot be unconfigured while it is being used by the server farm or firewall farm.

You can configure more than one probe, in any combination of supported types, for each server farm or for each firewall in a firewall farm.

Examples

The following example configures an IOS Server Load Balancing (IOS SLB) probe named PROBE3, then enters WSP probe configuration mode:

```
Router(config)# ip slb probe PROBE3 wsp
```

Related Commands

Command	Description
show ip slb probe	Displays information about an IOS SLB probe.

ip slb replicate slave rate

To set the replication message rate for IOS Server Load Balancing (IOS SLB) slave replication, use the **ip slb replicate slave rate** command in global configuration mode. To restore the default rate, use the **no** form of this command.

ip slb replicate slave rate *rate*

no ip slb replicate slave rate *rate*

Syntax Description

rate	Replication message rate for IOS SLB slave replication, in messages per second. The valid range is 50 messages per second to 1000 messages per second. The default setting is 400 messages per second.

Defaults

The default rate is 400 messages per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables you to manage Interprocess Communication Channel (IPC) resources between two route processors. If there is congestion between the two route processors, use this command to set a lower rate.

If the replication rate is exceeded, IOS SLB issues an appropriate error message.

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **ip slb replicate slave rate** command in global configuration mode.

The Home Agent Director does not support the **ip slb replicate slave rate** command in global configuration mode.

Examples

The following example sets the replication message rate to 500 messages per second:

```
Router(config)# ip slb replicate slave rate 500
```

Related Commands

Command	Description
replicate casa (firewall farm)	Configures a stateful backup of IOS SLB decision tables to a backup switch
replicate interval (firewall farm)	Sets the replication delivery interval for an IOS SLB firewall farm.
replicate slave (firewall farm)	Enables stateful backup of redundant route processors for an IOS SLBfirewall farm.
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb virtuals	Displays information about the virtual servers defined to IOS SLB.

ip slb route

To enable IOS Server Load Balancing (IOS SLB) to route packets using the RADIUS framed-IP sticky database, or to route packets from one firewall real server back through another firewall real server, use the **ip slb route** command in global configuration mode. To route packets normally, use the **no** form of this command.

ip slb route {**framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall**}

no ip slb route {**framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall**}

Syntax Description

framed-ip deny	(Optional) Packets that do not match entries in the IOS SLB RADIUS framed-ip sticky database are not routed.
ip-address	(Optional) IP address of packets to be inspected.
netmask	(Optional) Subnet mask specifying a range of packets to be inspected.
framed-ip	(Optional) Packets are to be routed using the IOS SLB RADIUS framed-IP sticky database.
inter-firewall	(Optional) Enables IOS SLB to route packets from one firewall real server back through another firewall real server, if the flows to the destination IP would otherwise have been firewall load-balanced. This can be done within the same firewall farm or across different firewall farms.

Defaults

Cisco IOS SLB cannot route packets using the RADIUS framed-IP sticky database, nor can it route packets from one firewall real server back through another firewall real server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **inter-firewall** keyword was added.
12.2 (14)ZA6	The **framed-ip deny** keyword was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables IOS SLB to inspect packets whose source IP addresses match the specified IP address and subnet mask. IOS SLB then searches for the packet's source IP address in the RADIUS framed-IP sticky database. If the database contains a matching entry, IOS SLB routes the packet to the associated real server. If the database does not contain a matching entry, IOS SLB routes the packet normally.

The **inter-firewall** keyword is useful when traffic is arriving from an address behind a firewall, is destined for an address behind a firewall, and has a sticky entry to be routed via the routing table.

Examples

The following example enables IOS SLB to inspect packets with the source IP address 10.10.10.1:

```
Router(config)# ip slb route 10.10.10.1 255.255.255.255 framed-ip
```

Related Commands

Command	Description
show ip slb sticky	Displays the IOS SLB sticky database.

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 Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

ip slb serverfarm *server-farm*

no ip slb serverfarm *server-farm*

Syntax Description

server-farm	Character string used to identify the server farm. The character string is limited to 15 characters.

Defaults

No server farm is identified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Grouping real servers into server farms is an essential part of IOS SLB. Using server farms enables IOS SLB to assign new connections to the real servers based on their weighted capacities, and on the load-balancing algorithms used.

Examples

The following example identifies a server farm named PUBLIC:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)#
```

Related Commands

Command	Description
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.

ip slb static

To configure a real server's Network Address Translation (NAT) behavior and enter static NAT configuration mode, use the **ip slb static** command in global configuration mode. To restore the real server's default NAT behavior, use the **no** form of this command.

ip slb static {**drop** | **nat** {**virtual** | *virtual-ip* [**per-packet** | **sticky**]}}

no ip slb static {**drop** | **nat** {**virtual** | *virtual-ip* [**per-packet** | **sticky**]}}

Syntax Description

drop	Indicates that IOS Server Load Balancing (IOS SLB) is to drop packets from this real server if the packets do not correspond to existing connections. This option is usually used in conjunction with the subnet mask or port number option on the **real** command in static NAT configuration mode, such that IOS SLB builds connections to the specified subnet or port, and drops all other connections from the real server.
nat virtual	Configures the real server to use server NAT, and to use the virtual IP address that is configured on the **real** command in static NAT configuration mode when translating addresses.
nat *virtual-ip*	Configures the real server to use server NAT, and to use the specified virtual IP address when translating addresses.
per-packet	(Optional) IOS SLB is *not* to maintain connection state for packets originating from the real server. That is, IOS SLB is to use server NAT to redirect packets originating from the real server.
sticky	(Optional) Indicates that IOS SLB is *not* to maintain connection state for packets originating from the real server, *unless* those packets match a sticky object. That is, if IOS SLB can find a matching sticky object, it builds the connection. Otherwise, IOS SLB does not build the connection.

Defaults

If you do not specify either the **per-packet** or **sticky** keyword, IOS SLB maintains connection state for packets originating from the real server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you specify the *virtual-ip* argument and you do not specify the **per-packet** option, IOS SLB uses server port translation to distinguish between connection requests initiated by different real servers.

Static NAT with the **per-packet** option specified does not load-balance fragmented packets.

Examples

The following example specifies that the real server is to use server NAT and to use virtual IP address 10.1.10.1 when translating addresses, and that IOS SLB is not to maintain connection state for any packets originating from the real server:

```
Router(config)# ip slb static nat 10.1.10.1 per-packet
```

Related Commands

Command	Description
show ip slb static	Displays information about the static NAT configuration.

ip slb timers gtp gsn

To change the amount of time IOS Server Load Balancing (IOS SLB) maintains sessions to and from an idle gateway general packet radio service (GPRS) support node (GGSN) or serving GPRS support node (SGSN), use the **ip slb timers gtp gsn** command in global configuration mode. To restore the default GPRS support node (GSN) idle timer, use the **no** form of this command.

ip slb timers gtp gsn *duration*

no ip slb timers gtp gsn *duration*

Syntax Description

duration	GSN idle timer duration in seconds, which defines how long IOS SLB is to allow a GGSN or SGSN to be idle (that is, to go without echoing or signaling through IOS SLB). When the timer expires, IOS SLB cleans up all sessions that are using the idle GGSN or SGSN. The valid range is 1 to 65535 seconds. The default value is 90 seconds.

Defaults

The default duration is 90 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command sets the GSN idle timer for all IOS SLB virtual servers that are configured for GPRS Tunneling Protocol (GTP) cause code inspection. When the GSN idle timer expires, IOS SLB destroys all sessions to and from the idle GGSN or SGSN.

Examples

The following example specifies that IOS SLB maintains sessions for 45 seconds after a GGSN or SGSN becomes idle:

```
Router(config)# ip slb timers gtp gsn 45
```

Related Commands

Command	Description
virtual	Configures the virtual server attributes.

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 Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

ip slb vserver *virtual-server*

no ip slb vserver *virtual-server*

Syntax Description

virtual-server	Character string used to identify the virtual server. The character string is limited to 15 characters.

Defaults

No virtual server is identified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example identifies a virtual server named PUBLIC_HTTP:

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

Related Commands

Command	Description
serverfarm	Associates a real server farm with a virtual server, and optionally configures a backup server farm and specifies that sticky connections are to be used in the backup server farm.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets going through a router, use the **ip tcp adjust-mss** command in interface configuration mode. To return the MSS value to the default setting, use the **no** form of this command.

ip tcp adjust-mss *max-segment-size*

no ip tcp adjust-mss *max-segment-size*

Syntax Description

max-segment-size	Maximum segment size, in bytes. The range is from 500 to 1460.

Command Default

The MSS is determined by the originating host.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was changed from **ip adjust-mss** to **ip tcp adjust-mss**.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZU2	This command was integrated into Cisco IOS Release 12.2(18)ZU2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When a host (usually a PC) initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the maximum transmission unit (MTU) configuration on the host. The default MSS value for a PC is 1500 bytes.

The PPP over Ethernet (PPPoE) standard supports an MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the Internet Control Message Protocol (ICMP) error messages that must be relayed from the host in order for path MTU to work.

The **ip tcp adjust-mss** command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The **ip tcp adjust-mss** command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

If you are configuring the **ip mtu** command on the same interface as the **ip tcp adjust-mss** command, we recommend that you use the following commands and values:

- **ip tcp adjust-mss 1452**
- **ip mtu 1492**

Examples

The following example shows the configuration of a PPPoE client with the MSS value set to 1452:

```
vpdn enable
no vpdn logging
!
vpdn-group 1
request-dialin
protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1 255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
 pppoe client dial-pool-number 1
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex B
dsl linerate AUTO
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 interface Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
access-list 101 permit ip 192.168.100.0 0.0.0.255 any
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.

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

Syntax Description

characters	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.

Defaults

0, which Telnet and rlogin interpret as the largest possible 32-bit positive number.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

It is unlikely you will need to change the default value.

Examples

The following example sets the maximum TCP read size to 64,000 bytes:

```
ip tcp chunk-size 64000
```

ip tcp compression-connections

To specify the total number of Transmission Control Protocol (TCP) header compression connections that can exist on an interface, use the **ip tcp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip tcp compression-connections *number*

no ip tcp compression-connections

Syntax Description

number	Number of TCP header compression connections the cache supports, in the range from 3 to 256.

Command Default

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You should configure one connection for each TCP connection through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.



Note Both ends of the serial connection must use the same number of cache entries.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

Related Commands

Command	Description
ip tcp header-compression	Enables TCP header compression.
show ip tcp header-compressions	Displays TCP header compression statistics.

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.

Command Default

TCP ECN is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following example shows how to enable TCP ECN:

```
ip tcp ecn
```

Related Commands

Command	Description
debug ip tcp ecn	Turns on TCP ECN debugging.
show tcp tcb	Displays the status of local and remote end hosts.

ip tcp header-compression

To enable Transmission Control Protocol (TCP) header compression, use the **ip tcp header-compression** command in interface configuration mode. To disable compression, use the **no** form of this command.

ip tcp header-compression [**passive | iphc-format | ietf-format**]

no ip tcp header-compression [**passive | iphc-format | ietf-format**]

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, all TCP packets are compressed.
iphc-format	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
ietf-format	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.

Command Default

Disabled

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format is as described in RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links.*

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was integrated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. This command was modified to include the **ietf-format** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. Compressing the TCP header can speed up Telnet connections dramatically.

In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on User Datagram Protocol (UDP) packets or other protocol headers.

The passive Keyword

By default, the **ip tcp header-compression** command compresses outgoing TCP traffic. If you specify the **passive** keyword, outgoing TCP traffic is compressed only if incoming TCP traffic on the same interface is compressed. If you do not specify the **passive** keyword, all outgoing TCP traffic is compressed.

For PPP interfaces, the **passive** keyword is ignored. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, Real-Time Transport Protocol (RTP) header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.



Note The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

The ietf-format Keyword

The **ietf-format** keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the **ietf-format** keyword compresses only TCP packets. For PPP interfaces, when the **ietf-format** keyword is specified, RTP header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.



Note The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format** keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
Router(config-if)# end
```

Related Commands

Command	Description
ip tcp compression-connections	Specifies the total number of TCP header compression connections that can exist on an interface.
show ip tcp header-compression	Displays TCP/IP header compression statistics.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

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 *bytes*

no ip tcp mss *bytes*

Syntax Description

bytes	Maximum segment size for TCP connections in bytes. Valid values are from 68 to 10000.

Defaults

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(05)S	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 nonlocal nodes.

Examples

The following example sets the MSS value at 250:

```
ip tcp mss 250
```

Related Commands

Command	Description
ip tcp header-compression	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

age-timer *minutes*	(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.
age-timer infinite	(Optional) Turns off the age timer.

Defaults

Disabled. If enabled, the minutes default is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
11.2	The **age-timer** and **infinite** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 reestimates 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

Syntax Description

packets	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.

Defaults

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.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Changing the default value changes the 5 segments, not the 20 segments.

Examples

The following example sets the maximum TCP outgoing queue to 10 packets:

```
ip tcp queuemax 10
```

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 (config)

Command History

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

Usage Guidelines

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
ip tcp header-compression	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*

Syntax Description

seconds	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.

Defaults

The default time is 30 seconds.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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.

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.

Examples

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 (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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
```

Related Commands

Command	Description
ip tcp header-compression	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 window size, use the **no** form of this command.

ip tcp window-size *bytes*

no ip tcp window-size

Syntax Description

bytes	Window size (in bytes). An integer from 0 to 1073741823. The default value is 4128. Window scaling is enabled when the window size is greater than 65535 bytes. **Note** As of Cisco IOS Release 15.0(1)M, the *bytes* argument can be set to an integer from 68 to 1073741823.

Command Default

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 65535 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.1	This command was introduced.
12.2(8)T	Default window size and maximum window scaling factor were increased.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified. The valid window size (in bytes) was changed to 68 to 1073741823.

Usage Guidelines

Do not use this command unless you clearly understand why you want to change the default value.

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.

The scale factor is automatically calculated based on the window-size that you configure. You cannot directly configure the scale factor.

Examples

The following example shows how to set the TCP window size to 1000 bytes:

```
ip tcp window-size 1000
```

ip unreachables

To enable the generation of Internet Control Message Protocol (ICMP) unreachable messages, use the **ip unreachables** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip unreachables

no ip unreachables

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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 unreachables
```

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
ip vrf vpn1
 rd 100:2
 route-target both 100:2
 route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (**interface configuration**)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf (tracking)

To track an IP route in a specific VPN virtual routing and forwarding (VRF) table, use the **ip vrf** command in tracking configuration mode. To remove the tracking of the route, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

The tracking of a route is not configured.

Command Modes

Tracking configuration (config-track)

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

Usage Guidelines

This command is available for all IP-route tracked objects that are tracked by the **track ip route** global configuration command. Use this command to track a route that belongs to a specific VPN.

Examples

In the following example, the route associated with a VRF named VRF1 is tracked:

```
Router(config)# track 1 ip route 10.0.0.0 255.0.0.0 metric threshold
Router(config-track)# exit
Router(config)# ip vrf VRF1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target both 100:1
!
Router(config)# interface ethernet0/2
Router(config-if)# no shutdown
Router(config-if)# ip vrf forwarding VRF1
Router(config-if)# ip address 10.0.0.2 255.0.0.0
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VPN VRF with an interface or subinterface.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

ip wccp

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, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**accelerated**] [**service-list** *service-access-list*] [**mode** {**open** | **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0** | **7**] *password*]

no ip wccp [**vrf** *vrf-name*]{**web-cache** | *service-number*}[**accelerated**] [**service-list** *service-access-list*] [**mode** {**open** | **closed**}] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0** | **7**] *password*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Specifies the web-cache service (WCCP version 1 and version 2). **Note** Web cache counts as one service. The maximum number of services, including those assigned with the *service-number* argument, are 256.
service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword. **Note** If Cisco cache engines are being used in your service group, the reverse-proxy service is indicated by a value of 99.
accelerated	(Optional) This option applies only to hardware-accelerated routers. This keyword configures the service group to prevent a connection being formed with a cache engine unless the cache engine is configured in a way that allows redirection on the router to benefit from hardware acceleration.
service-list *service-access-list*	(Optional) Identifies a named extended IP access list that defines the packets that will match the service.
open	(Optional) Identifies the service as open. This is the default service mode.
closed	(Optional) Identifies the service as closed.
group-address *multicast-address*	(Optional) Multicast IP address that communicates with the WCCP service group. The multicast address is used by the router to determine which web cache should receive redirected messages.
redirect-list *access-list*	(Optional) Access list that controls traffic redirected to this service group. The *access-list* argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.

group-list *access-list*	(Optional) Access list that determines which web caches are allowed to participate in the service group. The *access-list* argument specifies either the number or the name of a standard or extended access list.
password [**0** | **7**] *password*	(Optional) Message digest algorithm 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded. The encryption type can be 0 or 7, with 0 specifying not yet encrypted and 7 for proprietary. The *password* argument can be up to eight characters in length.

Command Default

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1	This command replaced the **ip wccp enable**, **ip wccp redirect-list**, and **ip wccp group-list** commands.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The maximum value for the *service-number* argument was increased to 254.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **service-list** *service-access-list* keyword and argument pair and the **mode open** and **mode closed** keywords were added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument pair were added.
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument pair were added.

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 should be enabled on the content engine interface, and the **ip wccp web-cache redirect out** command should be 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 configuration 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 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

The **vrf** *vrf-name* keyword and argument pair is optional. It allows you to specify a vrf to associate with a service group. You can then specify a web-cache service name or service number.

The same service (web-cache or service number) can be configured in different VRF tables. Each service will operate independently.

When the **no ip wccp** command is entered, the router terminates participation in the service group, deallocates space if none of the interfaces still has 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 [**vrf** *vrf-name*] {**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 [**vrf** *vrf-name*] {**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 the number or the name of a standard or extended 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 [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-list** *access-list*

This option instructs the router to use an access list to control the web caches that are allowed to participate in the specified service group. The *access-list* argument specifies either the number of a standard or extended access list or the name of any type of named 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 Application Services Command Reference*.

ip wccp [**vrf** *vrf-name*] {**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 eight 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.

ip wccp *service-number* **service-list** *service-access-list* **mode closed**

In applications where the interception and redirection of WCCP packet flows to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, it is necessary to block packet flows for the application when the intermediary device is not available. This blocking is called a closed service. By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device. The **service-list** keyword can only be used for closed mode services. When a WCCP service is configured as closed, WCCP discards packets that do not have a client application registered to receive the traffic. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When the definition of a service in a service list conflicts with the definition received via WCCP protocol, a warning message similar to the following is displayed:

```
Sep 28 14:06:35.923: %WCCP-5-SERVICEMISMATCH: Service 90 mismatched on WCCP client
10.1.1.13
```

When there is a conflict in service list definitions, the configured definition takes precedence over the external definition received via WCCP protocol messages.

Examples

The following example shows how to configure a router to run WCCP reverse-proxy service, using the multicast address of 239.0.0.0:

```
Router(config)# ip multicast-routing
Router(config)# ip wccp 99 group-address 239.0.0.0
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 group-listen
```

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:

```
Router(config)# access-list 100 deny ip any host 10.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache redirect out
```

The following example shows how to configure an access list to prevent traffic from network 10.0.0.0 leaving Fast Ethernet interface 0/0. Because the outbound ACL check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Router(config)# ip wccp web-cache
Router(config)# ip wccp check acl outbound
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 10 out
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config-if)# 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.

The following example shows how to configure a closed WCCP service:

```
Router(config)# ip wccp 99 service-list access1 mode closed
```

Related Commands

Command	Description
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP you wish to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ip wccp check acl outbound

To check the outbound access control list (ACL) for Web Cache Communication Protocol (WCCP), use the **ip wccp check acl outbound** command in global configuration mode. To disable the outbound check, use the **no** form of this command.

ip wccp check acl outbound

no ip wccp check acl outbound

Syntax Description

This command has no arguments or keywords.

Defaults

Check of the outbound ACL services is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S

Usage Guidelines

This command performs the same function as the **ip wccp outbound-acl-check** command.

Examples

The following example shows how to configure a router to check the outbound ACL for WCCP:

```
Router(config)# ip wccp check acl outbound
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
ip wccp check services all	Enables all WCCP services.
ip wccp outbound-acl-check	Checks the outbound ACL for WCCP.
ip wccp version	Specifies which version of WCCP to use on a router.

ip wccp check services all

To enable all Web Cache Communication Protocol (WCCP) services, use the **ip wccp check services all** command in global configuration mode. To disable all services, use the **no** form of this command.

ip wccp check services all

no ip wccp check services all

Syntax Description

This command has no arguments or keywords.

Defaults

WCCP services are not enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S

Usage Guidelines

With the **ip wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL access control list (ACL) as well as by the priority value of the service.

It is possible to configure an interface with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found which matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ip wccp check services all** command is configured. When the **ip wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

Note The priority of a WCCP service group is determined by the web cache appliance. The priority of a WCCP service group cannot be configured via Cisco IOS software.

Note The **ip wccp check services all** command is a global WCCP command that applies to all services and is not associated with a single service.

Examples

The following example shows how to configure all WCCP services:

```
Router(config)# ip wccp check services all
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
ip wccp version	Specifies which version of WCCP you wish to use on your router.

ip wccp enable

The **ip wccp enable** command 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 Web Cache Communication Protocol (WCCP), use the **ip wccp group-listen** command in interface configuration mode. To disable the reception of IP multicast packets for WCCP, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-listen**

no ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-listen**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Directs the router to send packets to the web cache service.
service-number	WCCP service number; valid values are from 0 to 254.

Defaults

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.1S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

Note To ensure correct operation on Catalyst 6500 series switches and Cisco 7600 series routers, you must enter the **ip pim** *mode* command in addition to the **ip wccp group-listen** command.

On Cisco 7600 series routers, the *service-number* may be either one of the provided standard keyword definitions or a number representing a cache engine dynamically defined definition. Once the service is enabled, the router can participate in the establishment of a service group.

On routers that are to be members of a Service Group when IP multicast is used, the following configuration is required:

- Configure the IP multicast address for use by the WCCP Service Group.
- Enable IP multicast routing using the **ip multicast-routing** command in global configuration mode.
- Configure the interfaces on which the router wishes to receive the IP multicast address with the **ip wccp** {**web-cache** | *service-number*} **group-listen** interface configuration command.

Examples

The following example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:

```
Router# configure terminal
Router(config)# ip multicast-routing
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache group-listen
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables WCCP redirection on an interface.

ip wccp outbound-acl-check

To check the outbound access control list (ACL) for Web Cache Communication Protocol (WCCP), use the **ip wccp outbound-acl-check** command in global configuration mode. To disable the outbound check, use the **no** form of this command.

ip wccp outbound-acl-check

no ip wccp outbound-acl-check

Syntax Description

This command has no arguments or keywords.

Command Default

Check of the outbound ACL services is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This command performs the same function as the **ip wccp check acl outbound** command.

Examples

The following example shows how to configure a router to chec the outbound ACL for WCCP:

```
Router(config)# ip wccp outbound-acl-check
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp check acl outbound	Checks the outbound ACL for WCCP.
ip wccp check services all	Enables all WCCP services.
ip wccp version	Specifies which version of WCCP to use on a router.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command in interface configuration mode. To disable WCCP redirection, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**in** | **out**}

no ip wccp [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**in** | **out**}

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
web-cache	Enables the web cache service.
service-number	Identification number of the cache engine service group controlled by a router; valid values are from 0 to 254. If Cisco cache engines are used in the cache cluster, the reverse proxy service is indicated by a value of 99.
in	Specifies packet redirection on an inbound interface.
out	Specifies packet redirection on an outbound interface.

Command Default

Redirection checking on the interface is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(11)S	The **in** keyword was added.
12.1(3)T	The **in** keyword was added.
12.2(17d)SXB	Support for this command on the Cisco 7600 series router Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 720.
12.2(18)SXF	This command was enhanced to support the Cisco 7600 series router Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. **Note** The **out** keyword is not supported in Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
12.2(33)SRE	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.1S	This command was modified. The **vrf** keyword and *vrf-name* argument were added. Support for the **out** keyword was added.

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 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 redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Tips Be careful not to confuse the **ip wccp redirect** {**out** | **in**} interface configuration command with the **ip wccp redirect exclude in** interface configuration command.

Note This command has the potential to affect 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 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 configuration, the multilink interface is configured to prevent the bypassing of NAT when fast/CEF switching is enabled:

```
Router(config)# interface multilink2
Router(config-if)# ip address 10.21.21.1 255.255.255.0
Router(config-if)# ip access-group IDS_Multilink2_in_1 in
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ip nat outside
Router(config-if)# ip inspect FSB-WALL out
Router(config-if)# max-reserved-bandwidth 100
Router(config-if)# service-policy output fsb-policy
Router(config-if)# no ip route-cache
Router(config-if)# load-interval 30
Router(config-if)# tx-ring-limit 3
Router(config-if)# tx-queue-limit 3
Router(config-if)# ids-service-module monitoring
```

```
Router(config-if)# ppp multilink
Router(config-if)# ppp multilink group 2
Router(config-if)# crypto map abc1
```

The following example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

The following example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 is redirected to a Cisco Cache Engine:

```
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
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
show ip interface	Displays the usability status of interfaces that are configured for IP.
show ip wccp	Displays the WCCP global configuration and statistics.

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.

Command Default

Redirection exclusion is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This configuration command instructs the interface to exclude inbound packets from any redirection check. Note that the command is global to all the services and should be applied to any inbound interface that will be excluded 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 Web Cache Communication Protocol (WCCP) v2 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
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.

ip wccp redirect-list

This command is now documented as part of the **ip wccp** command. See the description of the **ip wccp** command in this book for more information.

ip wccp source-interface

To specify the interface that Web Cache Communication Protocol (WCCP) uses as the preferred router ID and generic routing encapsulation (GRE) source address, use the **ip wccp source-interface** command in global configuration mode. To enable the WCCP default behavior for router ID selection, use the **no** form of this command.

ip wccp [**vrf** *vrf-name*] **source-interface** *source-interface*

no ip wccp [**vrf** *vrf-name*] **source-interface**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding instance (VRF) to associate with a service group.
source-interface	The type and number of the source interface.

Command Default

If this command is not configured, WCCP selects a loopback interface with the highest IP address as the router ID.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to set the interface from which WCCP may derive the router ID and GRE source address. The router ID must be a reachable IPv4 address.

The interface identified by the *source-interface* argument must be assigned an IPv4 address and be operational before WCCP uses the address as the router ID. If the configured source interface cannot be used to derive the WCCP router ID, a Cisco IOS error message similar to the following is displayed:

```
%WCCP-3-SIFIGNORED: source-interface interface ignored (reason)
```

The *reason* field in the error output indicates why the interface has been ignored and can include the following:

- **VRF mismatch**—The VRF domain associated with the interface does not match the VRF domain associated with the WCCP command.
- **interface does not exist**—The interface has been deleted.
- **no address**—The interface does not have a valid IPv4 address.
- **line protocol down**—The interface is not fully operational.

This command provides control only of the router ID and GRE source address. This command does not influence the source address used by WCCP control protocol (“Here I Am” and Removal Query messages). The WCCP control protocol is not bound to a specific interface and the source address is always selected based on the destination address of an individual packet.

Examples

The following example shows how to select Gigabit Ethernet interface 0/0/0 as the WCCP source interface:

```
Router(config)# ip wccp source-interface gigabitethernet0/0/0
```

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
show ip wccp	Displays the WCCP global configuration and statistics.
show ip wccp global counters	Displays global WCCP information for packets that are processed in software.
show platform software wccp	Displays platform specific configuration and statistics related WCCP information on Cisco ASR 1000 Series Routers.

ip wccp version

To specify the version of Web Cache Communication Protocol (WCCP), use the **ip wccp version** command in global configuration mode.

ip wccp version {**1** | **2**}

Syntax Description

1	Specifies Web Cache Communication Protocol Version 1 (WCCPv1).
2	Specifies Web Cache Communication Protocol Version 2 (WCCPv2).

Command Default

WCCPv2

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. Only WCCP version 2 is supported in Cisco IOS XE Release 2.2.

Usage Guidelines

Configuring this command does not have any impact on Cisco ASR 1000 Series Routers because these routers support only WCCPv2. WCCPv2 is enabled by default on Cisco ASR 1000 series routers when a service group is configured or a service group is attached to an interface.

Examples

In the following example, the user changes the WCCP version from the default of WCCPv2 to WCCPv1, starting in privileged EXEC mode:

```
Router(config)# ip wccp version 1

Router# show ip wccp

% WCCP version 2 is not enabled
```

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
show ip wccp	Displays the WCCP global configuration and statistics.

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated [[**group-address** *group-address*] | [**redirect-list** *access-list]* | [**group-list** *access-list*] | [**password** *password*]]

no ip wccp web-cache accelerated

Syntax Description

group-address *group-address*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Defaults

When this command is not configured, hardware acceleration for WCCPv1 is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **group-address** *group-address* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. 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. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all "Here I Am" messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access

list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. 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 specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.

kal-ap domain

To enable the IOS SLB KeepAlive Application Protocol (KAL-AP) agent to look for a domain tag when reporting the load for a virtual server, use the **kal-ap domain** command in server farm configuration mode. To delete the domain tag, use the **no** form of this command.

kal-ap domain *tag*

no kal-ap domain

Syntax Description

tag	1- to 64-character domain tag to be used by the KAL-AP agent. All characters are valid; case is significant.

Defaults

The KAL-AP agent does not look for a domain tag when reporting the load for a virtual server.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

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

Usage Guidelines

Configure the **kal-ap domain** command on the server farm that is associated with the virtual server for which the KAL-AP agent is to report the load.

Examples

The following example specifies that the KAL-AP agent is to look for domain tag **chicago.com**:

```
Router(config-slb-sfarm)# kal-ap domain chicago-com
```

Related Commands

Command	Description
ip capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.
ip slb serverfarm	Identifies a server farm and enter SLB server farm configuration mode.

lookup

To configure an IP address of a real server that a Domain Name System (DNS) server should supply in response to a domain name resolve request, use the **lookup** command in DNS probe configuration mode. To remove an IP address from the expected list, use the **no** form of this command.

lookup *ip-address*

no lookup *ip-address*

Syntax Description

ip-address	IP address of a real server that a DNS server should supply in response to a domain name resolve request.

Defaults

No lookup IP address is configured.

Command Modes

DNS probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a DNS probe named PROBE4, enters DNS probe configuration mode, and specifies 10.1.10.1 as the IP address to resolve:

```
Router(config)# ip slb probe PROBE4 dns
Router(config-slb-probe)# lookup 10.1.10.1
```

Related Commands

Command	Description
ip slb probe dns	Configures a DNS probe name and enters DNS probe configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

manager (DFP agent)

This command has been removed. Its function is now performed by the **ip dfp agent** global configuration command, and by the following DFP agent configuration commands:

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

See the description of these commands for more information.

maxclients

To specify the maximum number of IOS Server Load Balancing (IOS SLB) RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server, use the **maxclients** command in real server configuration mode. To remove the limit, use the **no** form of this command.

maxclients *maximum-number*

no maxclients

Syntax Description

maximum-number	Maximum number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server: • If the **radius calling-station-id** keyword is specified in the **sticky** command for the virtual server (that is, if the virtual server is configured to create the IOS SLB RADIUS calling-station-ID sticky database), a sticky subscriber is an entry in the IOS SLB RADIUS calling-station-ID sticky database. • If the **radius framed-ip** keyword is specified in the **sticky** command for the virtual server (that is, if the virtual server is configured to create the IOS SLB RADIUS framed-IP sticky database), a sticky subscriber is an entry in the IOS SLB RADIUS framed-IP sticky database. • If the **radius username** keyword is specified in the **sticky** command for the virtual server (that is, if the virtual server is configured to create the IOS SLB RADIUS username sticky database), a sticky subscriber is an entry in the IOS SLB RADIUS username sticky database. • If both the **radius framed-ip** and **radius calling-station-id** keywords are specified in the **sticky** command for the virtual server, a sticky subscriber is an entry in the IOS SLB RADIUS calling-station-ID sticky database. • If both the **radius framed-ip** and **radius username** keywords are specified in the **sticky** command for the virtual server, a sticky subscriber is an entry in the IOS SLB RADIUS username sticky database. By default, there is no limit on the number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server.

Defaults

There is no limit on the number of IOS SLB RADIUS and GTP sticky subscribers that can be assigned to an individual virtual server.

Command Modes

Real server configuration (config-slb-real)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.1(12c)E	This command was modified to support RADIUS load balancing for CDMA2000, a third-generation (3-G) version of Code Division Multiple Access (CDMA).
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that up to 10 IOS SLB RADIUS sticky subscribers can be assigned to an individual real server:

```
Router(config-slb-real)# maxclients 10
```

Related Commands

Command	Description
ip slb route	Enables IOS SLB to inspect packets for RADIUS framed-IP sticky routing.
show ip slb sticky	Displays the IOS SLB sticky database.

maxconns (firewall farm datagram protocol)

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

maxconns *maximum-number*

no maxconns

Syntax Description

maximum-number	Maximum number of simultaneous active datagram connections using the firewall farm. Valid values range from 1 to 4294967295. The default is 4294967295.

Defaults

The default maximum number of simultaneous active datagram connections using the firewall farm is 4294967295.

Command Modes

Firewall farm datagram protocol configuration (config-slb-fw-udp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
Router(config-slb-fw-udp)# maxconns 1000
```

Related Commands

Command	Description
protocol datagram	Enters firewall farm datagram protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb reals	Displays information about the real servers.

maxconns (firewall farm TCP protocol)

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

maxconns *maximum-number*

no maxconns

Syntax Description

maximum-number	Maximum number of simultaneous active TCP connections using the firewall farm. Valid values range from 1 to 4294967295. The default is 4294967295.

Defaults

The default maximum number of simultaneous active TCP connections using the firewall farm is 4294967295.

Command Modes

Firewall farm TCP protocol configuration (config-slb-fw-tcp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# maxconns 1000
```

Related Commands

Command	Description
protocol tcp	Enters firewall farm TCP protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb reals	Displays information about the real servers.

maxconns (server farm)

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

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

no maxconns

Syntax Description

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

Defaults

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

Command Modes

SLB server farm configuration (config-slb-real)

Command History

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

Examples

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

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

Related Commands

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

mls aging slb normal

To configure the aging time for flows, use the **mls aging slb normal** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls aging slb normal *time*

no mls aging slb normal *time*

Syntax Description

time	Idle time, in milliseconds, before a flow is aged. The valid range is 1 milliseconds to 10000 milliseconds. The default setting is 2000 milliseconds. **Note** Heavier-than-normal loads can age flows more aggressively than this time.

Defaults

The default aging idle time is 2000 milliseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(8)E	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported for Catalyst 6000 family switches only.

Examples

The following example sets the idle time to 4000 milliseconds:

```
Router(config)# mls aging slb normal 4000
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall farm and initiates firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.
mls aging slb process	Controls how often the aging process runs.

mls aging slb process

To control how often the aging process runs, use the **mls aging slb process** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls aging slb process *time*

no mls aging slb process *time*

Syntax Description

time	Aging process interval, in milliseconds. The valid range is 1 millisecond to 10000 milliseconds. The default setting is 2000 seconds.

Defaults

The default aging process interval is 2000 milliseconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(8)E	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported for Catalyst 6000 family switches only.

Examples

The following example sets the aging process interval to 4000 milliseconds:

```
Router(config)# mls aging slb process 4000
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall farm and initiates firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.
mls aging slb normal	Configures the aging time for flows.

mls ip install-threshold

To install the configured ACL thresholds, use the **mls ip install-threshold** command in global configuration mode.

mls ip install-threshold *acl-num*

Syntax Description

acl-num	Reflective ACL number; valid values are from 1 to 10000.

Defaults

This command has no default settings.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

The **mls ip install-threshold** command is active only when you enable the **mls ip reflexive ndr-entry tcam** command.

Examples

This example shows how to install an ACL threshold:

```
Router(config)# mls ip install-threshold 123
```

Related Commands

Command	Description
mls ip delete-threshold	Deletes configured ACL thresholds.
mls ip reflexive ndr-entry tcam	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.

mls ip reflexive ndr-entry tcam

To enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **mls ip reflexive ndr-entry tcam** command in global configuration mode. To disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR, use the **no** form of this command.

mls ip reflexive ndr-entry tcam

no mls ip reflexive ndr-entry tcam

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on Cisco 7600 series routers that are configured with a Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

When you enter the **mls ip reflexive ndr-entry tcam** command, the reflexive ACL dynamic entries are installed in TCAM instead of in NetFlow.

Examples

This example shows how to enable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# mls ip reflexive ndr-entry tcam
```

This example shows how to disable the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR:

```
Router(config)# no mls ip reflexive ndr-entry tcam
```

Related Commands

Command	Description
mls ip delete-threshold	Deletes configured ACL thresholds.
mls ip install-threshold	Installs the configured ACL thresholds.

mls ip slb purge global

To specify protocol-level purging of MLS entries from active TCP and UDP flow packets, use the **mls ip slb purge global** command in global configuration mode. To disable purge throttling, use the **no** form of this command.

mls ip slb purge global

no mls ip slb purge global

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is for protocol-level purging.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(1)SX	This command was introduced.
12.2(33)SRD2	The command was modified so that the default command no longer appears in the generated configuration.
12.2(33)SXI2	The command was modified so that the default command no longer appears in the generated configuration.
12.2(18)SXF17	The command was modified so that the default command no longer appears in the generated configuration.

Examples

The following example disables purge throttling on TCP and UDP flow packets:

```
Router(config)# no mls ip slb purge global
Router(config)#
```

The following example returns purge throttling on TCP and UDP flow packets to its default setting:

```
Router(config)# mls ip slb purge global
Router(config)#
```

mls ip slb search wildcard

To specify the behavior of IOS Server Load Balancing (IOS SLB) wildcard searches, use the **mls ip slb search wildcard** command in global configuration mode. To restore the default setting, use the **no** form of this command.

mls ip slb search {**wildcard** [**pfc** | **rp**] | **icmp**}

no mls ip slb search {**wildcard** [**pfc** | **rp**] | **icmp**}

Syntax Description

wildcard	IOS SLB wildcard searches are to be performed by the Policy Feature Card (PFC). This value is the default setting.
pfc	(Optional) IOS SLB wildcard searches are to be performed by the Policy Feature Card (PFC). This value is the default setting.
rp	(Optional) IOS SLB wildcard searches are to be performed by the route processor.
icmp	Disables ICMP handling by IOS SLB. (Pings to IOS SLB virtual IP addresses are still answered.) Use this command to reduce CPU usage when IOS SLB is configured in locations with a high volume of ICMP flows, such as in the network core. **Note** Use of the **icmp** keyword can result in minor ICMP errors, such as flows returned to the client with no Network Address Translation (NAT).

Defaults

The default setting is for the PFC to perform IOS SLB wildcard searches.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported for Catalyst 6500 family switches only.

If you configure IOS SLB and either input ACLs or firewall load balancing on the same Catalyst 6500 Family Switch, you can exceed the capacity of the TCAM on the PFC. To correct the problem, use the **mls ip slb search wildcard rp** command to reduce the amount of TCAM space used by IOS SLB. However, be aware that this command can result in a slight increase in route processor utilization.

Examples

The following example limits wildcard searches to the route processor:

```
Router(config)# mls ip slb search wildcard rp
```

Related Commands

Command	Description
ip slb firewallfarm	Identifies a firewall by IP address farm and enters firewall farm configuration mode.
ip slb serverfarm	Associates a real server farm with a virtual server.
ip slb vserver	Identifies a virtual server.

nat

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

nat {**client** *pool* | **server**}

no nat {**client** | **server**}

Syntax Description

client *pool*	Configures the client address in load-balanced packets using addresses from the client address pool. The pool name must match the *pool* argument from a previous **ip slb natpool** command. This mode is commonly referred to as *directed client NAT*, or simply client NAT.
server	Configures the destination address in load-balanced packets sent to the real server as the address of the real server chosen by the server farm load-balancing algorithm. This mode is commonly referred to as *directed server NAT*, or simply server NAT.

Defaults

No IOS SLB NAT is configured.

Command Modes

SLB server farm configuration (config-slb-sfarm)

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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(2)E	The **client** keyword and *pool* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

Examples

The following example enters server farm configuration mode and configures NAT mode as server address translation on server farm FARM2:

```
Router# ip slb serverfarm FARM2
Router(config-slb-sfarm)# nat server
```

The following example configures the NAT mode on server farm FARM2 to client translation mode and, using the **real** command in server farm configuration mode, configures the real server IP address as 10.3.1.1:

```
Router(config-slb-sfarm)# nat client web-clients
Router(config-slb-sfarm)# real 10.3.1.1
```

Related Commands

Command	Description
ip slb serverfarm	Associates a real server farm with a virtual server.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb serverfarms	Displays information about the server farm configuration.

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

object-number	Object in a tracked list of objects. The range is from 1 to 1000.
not	(Optional) Negates the state of an object. **Note** The **not** keyword cannot be used in a weight or percentage threshold list. It can only be used in a Boolean list.
weight *weight-number*	(Optional) Specifies a threshold weight for each object.

Command Default

The object is not included in the tracked list.

Command Modes

Tracking configuration (config-track)

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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows two serial interfaces (objects) that are in tracked list 100. The Boolean "not" negates the state of object 2, resulting in the tracked list regarding object 2 as down when it is up.

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
```

```
Router(config)# track 100 list boolean and
Router(config-track)# object 1
Router(config-track)# object 2 not
```

Related Commands

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

password (DFP agent)

To configure a Dynamic Feedback Protocol (DFP) agent password for Message Digest Algorithm Version 5 (MD5) authentication, use the **password** command in DFP agent configuration mode. To remove the DFP agent password, use the **no** form of this command.

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

no password

Syntax Description

0	(Optional) Indicates that the password is unencrypted. This is the default setting.
7	(Optional) Indicates that the password is encrypted.
password	Password value for MD5 authentication. **Note** This password must match the password configured on the host agent.
timeout	(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

The password encryption default is 0 (unencrypted).
The password timeout default is 180 seconds.

Command Modes

DFP agent configuration (config-dfp)

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.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The password specified on this command must match the password specified on the DFP manager.

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. Setting a longer timeout 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.

If you are running IOS SLB as a DFP manager, and you specify a password on the **ip slb dfp** command in global configuration mode, the password must match the one specified on the **password** command in DFP agent configuration mode in the DFP agent.

Examples

The following example sets the DFP agent password (unencrypted by default) to Password1 and the timeout to 360 seconds:

```
Router(config)# ip dfp agent slb
Router(config-dfp)# password Password1 360
```

Related Commands

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

peer port

To specify the port to which the IOS SLB KeepAlive Application Protocol (KAL-AP) agent is to connect, use the **peer port** command in SLB Content Application Peering Protocol (CAPP) configuration mode. To restore the default settings, use the **no** form of this command.

peer [*ip-address*] **port** *port*

no peer [*ip-address*] **port** *port*

Syntax Description

ip-address	(Optional) IP address of the peer KAL-AP manager.
port	Content Application Peering Protocol (CAPP) User Datagram Protocol (UDP) port number to which the KAL-AP agent is to connect. Valid port numbers are 1 to 65535.

Defaults

If you do not specify a port, the KAL-AP agent connects to port 5002.

Command Modes

SLB CAPP configuration (config-slb-capp)

Command History

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

Usage Guidelines

Use this command to specify a port number, other than port 5002, to be used by the KAL-AP agent.

You can configure any number of **peer port** commands with the *ip-address* argument, but only one without the *ip-address* argument.

Examples

The following example configures the KAL-AP agent to connect to port number 6000:

```
Router(config-slb-capp)# peer port 6000
```

Related Commands

Command	Description
ip capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.

peer secret

To enable Message Digest Algorithm Version 5 (MD5) authentication for the IOS SLB KeepAlive Application Protocol (KAL-AP) agent, use the **peer secret** command in SLB Content Application Peering Protocol (CAPP) configuration mode. To disable MD5 authentication, use the **no** form of this command.

peer [*ip-address*] **secret** [*encrypt*] *secret-string*

no peer [*ip-address*] **secret** *secret-string*

Syntax Description

ip-address	(Optional) IP address of the peer KAL-AP.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the KAL-AP client.

Defaults

The KAL-AP agent does not use MD5 authentication with IOS SLB.

Command Modes

SLB CAPP configuration (config-slb-capp)

Command History

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

Usage Guidelines

You can configure any number of **peer secret** commands with the *ip-address* argument, but only one without the *ip-address* argument.

Examples

The following example configures secret string SECRET_STRING for the KAL-AP agent:

```
Router(config-slb-capp)# peer secret SECRET_STRING
```

Related Commands

Command	Description
ip capp udp	Enables the IOS SLB KeepAlive Application Protocol (KAL-AP) agent and enters SLB Content Application Peering Protocol (CAPP) configuration mode.

platform trace runtime process forwarding-manager module wccp

To enable Forwarding Manager Route Processor and Embedded-Service-Processor trace messages for the Web Cache Communication Protocol (WCCP) process, use the **platform trace runtime process forwarding-manager module wccp** command in global configuration mode. To disable debug messages, use the **no** form of this command.

platform trace runtime slot *slot* **bay** *bay* **process forwarding-manager module wccp level** {*level*}

no platform trace runtime slot *slot* **bay** *bay* **process forwarding-manager module wccp**

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: • **F0**—Embedded Service Processor slot 0 • **R0**—Route Processor slot 0 • **F1**—Embedded Service Processor slot 1 • **R1**—Route Processor slot 1
bay	Chassis bay to configure. Valid options are: • **0** • **1**
level *level*	Selects the trace level. The trace level determines how much information about a module should be stored in the trace buffer or file. Valid options are: • **debug**—Provides debug-level output. • **emergency**—Provides information about an issue that makes the system unusable. • **error**—Provides information about a system error. • **info**—Informational purposes only. • **noise**—All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. • **notice**—Provides information regarding a significant issue, but the router is still working normally. • **verbose**—All possible tracing messages are sent. • **warning**—Provides information about a system warning.

Command Default

The default tracing level for every module on the Cisco ASR 1000 Series Routers is notice.

Command Modes Global configuration (config)

Command History

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

Usage Guidelines Trace level settings are leveled: every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3 (error) ensures that the trace file contains all output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) ensures that all trace output for the specific module is included in that trace file.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.

When setting trace levels, it is also important to remember that the setting is not done in a configuration mode, so trace level settings are returned to their defaults after every router reload.

Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to the debug level or higher should be done with discretion.

Caution Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples In the following example, the trace level for the WCCP module in the Forwarding Manager of the ESP processor in slot 0 is set to the informational tracing level (info):

```
Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module
wccp level info
```

Related Commands

Command	Description
show platform software trace level	Displays trace levels for specified modules.
show platform software trace message	Displays trace messages.

port (custom UDP probe)

To specify the port to which a custom User Datagram Protocol (UDP) probe is to connect, use the **port** command in custom UDP probe configuration mode. To restore the default settings, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	UDP port number to which the custom UDP probe is to connect.

Defaults

In dispatched mode, the port number is inherited from the virtual server.
If port translation is configured for the real server, that port number is used. See the **real (server farm)** command for more details.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a custom UDP probe named PROBE6, enters custom UDP probe configuration mode, and configures the probe to connect to port number 8:

```
Router(config)# ip slb probe PROBE6 custom UDP
Router(config-slb-probe)# port 8
```

Related Commands

Command	Description
ip slb probe custom udp	Configures a custom User Datagram Protocol (UDP) probe name and enters custom UDP probe configuration mode.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

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*

Syntax Description

port-number	Port number used by a DFP manager to connect to a DFP agent. The valid range is from 1 to 65535.

Defaults

No port number is defined.

Command Modes

DFP agent configuration (config-dfp)

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.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

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

Related Commands

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

port (HTTP probe)

To specify the port to which an HTTP probe is to connect, use the **port** command in HTTP probe configuration mode. To restore the default settings, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	TCP or User Datagram Protocol (UDP) port number to which the HTTP probe is to connect.

Defaults

In dispatched mode, the port number is inherited from the virtual server.
If port translation is configured for the real server, that port number is used. See the **real** (server farm) command for more details.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures an HTTP probe named PROBE2, enters HTTP probe configuration mode, and configures the probe to connect to port number 8:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# port 8
```

Related Commands

Command	Description
ip slb probe http	Configures an HTTP probe name and enters HTTP probe configuration mode.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

port (TCP probe)

To specify the port to which a TCP probe is to connect, use the **port** command in TCP probe configuration mode. To restore the default settings, use the **no** form of this command.

port *port*

no port *port*

Syntax Description

port	TCP port number to which the TCP probe is to connect.

Defaults

In dispatched mode, the port number is inherited from the virtual server.
If port translation is configured for the real server, that port number is used. See the **real** (server farm) command for more details.

Command Modes

TCP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a TCP probe named PROBE5, enters TCP probe configuration mode, and configures the probe to connect to port number 8:

```
Router(config)# ip slb probe PROBE5 tcp
Router(config-slb-probe)# port 8
```

Related Commands

Command	Description
ip slb probe tcp	Configures a TCP probe name and enters TCP probe configuration mode.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb probe	Displays information about an IOS SLB probe.

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** | **route-map** *mapname*]

no predictor

Syntax Description

roundrobin	(Optional) Uses the weighted round robin algorithm for selecting the real server to handle the next new connection for the server farm. See the "Weighted Round Robin" section for a detailed description of this algorithm. This algorithm is the default value. RADIUS load balancing requires the weighted round robin algorithm. General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled requires the weighted round robin algorithm. The Home Agent Director requires the weighted round robin algorithm.
leastconns	(Optional) Uses the weighted least connections algorithm for selecting the real server to handle the next new connection for this server farm. See the "Weighted Least Connections" section for a detailed description of this algorithm.
route-map *mapname*	(Optional) Uses IOS policy-based routing (PBR) for selecting the real server to handle the next new connection for this server farm. The *mapname* argument identifies the IOS PBR route map to be used. See the "Route Map" section for a detailed description of this algorithm. The route map algorithm is supported only for RADIUS load balancing accelerated data plane forwarding.

Defaults

If you do not enter a **predictor** command, or if you enter the **predictor** command without specifying a load-balancing algorithm, the weighted round robin algorithm is used.

Command Modes

SLB server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **route-map** keyword and *mapname* argument were added.

Usage Guidelines

RADIUS load balancing requires the weighted round robin algorithm.

The route map algorithm is supported only for RADIUS load balancing accelerated data plane forwarding. When you specify the **predictor route-map** command, no further commands in SLB server farm configuration mode or real server configuration mode are allowed.

GPRS load balancing without GTP cause code inspection enabled requires the weighted round robin algorithm. A server farm that uses weighted least connections can be bound to a virtual server providing GPRS load balancing without GTP cause code inspection enabled, but you cannot place the virtual server INSERVICE. If you try to do so, Cisco IOS SLB) issues an error message.

The Home Agent Director requires the weighted round robin algorithm. A server farm that uses weighted least connections can be bound to a Home Agent Director virtual server, but you cannot place the virtual server INSERVICE. If you try to do so, Cisco IOS SLB issues an error message.

Examples

The following example specifies the weighted least connections algorithm:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# predictor leastconns
```

Related Commands

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

predictor hash address (firewall farm)

To specify the load-balancing algorithm for selecting a firewall in the firewall farm, use the **predictor hash address** command in firewall farm configuration mode. To restore the default load-balancing algorithm, use the **no** form of this command.

predictor hash address [**port**]

no predictor

Syntax Description

port	(Optional) Uses the source and destination TCP or User Datagram Protocol (UDP) port numbers, in addition to the source and destination IP addresses, when selecting a firewall.

Defaults

IOS Server Load Balancing (IOS SLB) uses the source and destination IP addresses when selecting a firewall.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that source and destination IP addresses are to be used when selecting a firewall:

```
Router(config)# ip slb firewall FIRE1
Router(config-slb-fw)# predictor hash address
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.
weight (firewall farm real server)	Specifies the firewall's capacity, relative to other firewalls in the firewall farm.

probe (firewall farm real server)

To associate a probe with a firewall farm, use the **probe** command in firewall farm real server configuration mode. To remove the association, use the **no** form of this command.

probe *probe*

no probe *probe*

Syntax Description

probe	Name of the probe to associate with this firewall farm.

Defaults

No probe is associated with a firewall farm.

Command Modes

Firewall farm real server configuration (config-slb-fw-real)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure more than one probe for each firewall in a firewall farm.

If you configure probes in your network, you must also do one of the following:

- Configure the **exclude** keyword on the **client** command on the virtual server, to exclude connections initiated by the client IP address from the load-balancing scheme.
- Configure IP addresses on the IOS Server Load Balancing (IOS SLB) device that are Layer 3-adjacent to the real servers used by the virtual server.

Examples

The following example associates probe FireProbe with server farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw-real)# probe FireProbe
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the server farm configuration.

probe (server farm)

To associate a probe with a server farm, use the **probe** command in server farm configuration mode. To remove the association, use the **no** form of this command.

probe *probe*

no probe *probe*

Syntax Description

probe	Name of the probe to associate with this server farm.

Defaults

No probe is associated with a server farm.

Command Modes

Server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure more than one probe for each server farm.

If you configure probes in your network, you must also do one of the following:

- Configure the **exclude** keyword on the **client** command on the virtual server, to exclude connections initiated by the client IP address from the load-balancing scheme.
- Configure IP addresses on the IOS Server Load Balancing (IOS SLB) device that are Layer 3-adjacent to the real servers used by the virtual server.

Examples

The following example associates probe PROBE1 with server farm PUBLIC:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# probe PROBE1
```

Related Commands

Command	Description
show ip slb serverfarms	Displays information about the server farm configuration.

protocol datagram

To enter firewall farm datagram protocol configuration mode, use the **protocol datagram** command in firewall farm configuration mode.

protocol datagram

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(11b)E	This command was introduced, replacing the **udp** command.
12.1(12c)E	This command was integrated into Cisco IOS Release 12.1(12c)E, replacing the **protocol udp** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Firewall farm datagram protocol configuration applies to the Encapsulation Security Payload (ESP), Generic Routing Encapsulation (GRE), IP in IP encapsulation, and User Datagram Protocol (UDP) protocols.

Examples

The following example enters firewall farm datagram protocol configuration mode:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

protocol tcp

To enter firewall farm TCP protocol configuration mode, use the **protocol tcp** command in firewall farm configuration mode.

protocol tcp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(11b)E	This command was introduced, replacing the **tcp** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example enters firewall farm TCP protocol configuration mode:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.

purge connection

To enable IOS SLB firewall load balancing to send purge requests for connections, use the **purge connection** command in firewall farm configuration mode. To prevent the sending of purge requests, use the **no** form of this command.

purge connection

no purge connection

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB firewall load balancing sends purge requests for connections.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

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

Usage Guidelines

By default, IOS SLB firewall load balancing sends purge requests for connections. However, if a large number of purge requests are sent, the CPU might be impacted. To prevent this problem, use the **no** form of this command to prevent the sending of purge requests.

Examples

The following example prevents the sending of purge requests for connections:

```
Router(config-slb-fw)# no purge connection
```

Related Commands

mls ip slb purge global	Specifies protocol-level purging of MLS entries from active TCP and UDP flow packets.
purge sticky	TBD

purge radius framed-ip acct on-off

To enable IOS SLB to purge entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting ON or OFF message, use the **purge radius framed-ip acct on-off** command in virtual server configuration mode. To disable this behavior, use the **no** form of this command.

purge radius framed-ip acct on-off

no purge radius framed-ip acct on-off

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB purges entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting ON or OFF message.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example prevents IOS SLB from purging entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting ON or OFF message:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# no purge radius framed-ip acct on-off
```

Related Commands

Command	Description
sticky (virtual server)	Assigns all connections from a client to the same real server.

purge radius framed-ip acct stop

To enable IOS Server Load Balancing to purge entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting-Stop message, use the **purge radius framed-ip acct stop** in virtual server configuration mode. To disable this behavior, use the **no** form of this command.

purge radius framed-ip acct stop {*attribute-number* | **26** | **vsa** {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*}

no purge radius framed-ip acct stop {*attribute-number* | **26** | **vsa** {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*}

Syntax Description

attribute-number	RADIUS attribute number.
26	RADIUS attribute number 26.
vsa	Vendor-specific attribute number.
vendor-ID	Vendor ID.
3gpp	Third Generation Partnership Project (3GPP) vendor ID.
3gpp2	Third Generation Partnership Project 2 (3GPP2) vendor ID.
sub-attribute-number	Sub-attribute number.

Defaults

IOS SLB purges entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting-Stop message.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example prevents IOS SLB from purging entries in the IOS SLB RADIUS framed-ip sticky database upon receipt of an Accounting-Stop message:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# no purge radius framed-ip acct stop 44
```

Related Commands

Command	Description
sticky (virtual server)	Assigns all connections from a client to the same real server.

purge sticky

To enable IOS SLB firewall load balancing to send purge requests for sticky connections when the sticky timer expires, use the **purge sticky** command in firewall farm configuration mode. To prevent the sending of purge requests when the timer expires, use the **no** form of this command.

purge sticky

no purge sticky

Syntax Description

This command has no arguments or keywords.

Defaults

IOS SLB firewall load balancing sends purge requests when the sticky timer expires.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

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

Usage Guidelines

By default, IOS SLB firewall load balancing sends purge requests for sticky connections when the sticky timer expires. However, large volumes of purge requests can impact the CPU. To prevent this problem, use the **no** form of this command to prevent the sending of purge requests when the sticky timer expires.

To configure a sticky timer for IOS SLB firewall load balancing, use the **sticky** command in either firewall farm datagram protocol or firewall farm TCP protocol configuration mode.

Examples

The following example prevents the sending of purge requests for sticky connections:

```
Router(config-slb-fw)# no purge sticky
```

Related Commands

mls ip slb purge global	Specifies protocol-level purging of MLS entries from active TCP and UDP flow packets.
purge connection	Enables IOS SLB firewall load balancing to send purge requests for connections.
sticky (firewall farm datagram protocol)	Assigns all connections from a client to the same firewall.
sticky (firewall farm TCP protocol)	Assigns all connections from a client to the same firewall.

radius acct local-ack key

To enable a RADIUS virtual server to acknowledge RADIUS accounting messages, use the **radius acct local-ack key** command in SLB virtual server configuration mode. To restore the default behavior, use the **no** form of this command.

radius acct local-ack key [*encrypt*] *secret-string*

no radius acct local-ack key [*encrypt*] *secret-string*

Syntax Description

encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).

Defaults

By default, this command is not enabled. When this command is enabled, the RADIUS load balancing device, not the real server, acknowledges RADIUS accounting messages.
If you configure this command but you do not specify the **7** keyword, the *secret-string* is stored in the plain text.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

Configure this command only on a RADIUS virtual server.

Examples

The following example shows how to enable RADIUS virtual server PUBLIC_RADIUS to acknowledge RADIUS accounting messages with key SECRET_PASSWORD.

```
Router(config)# ip slb vserver PUBLIC_RADIUS
Router(config-slb-vserver)# radius acct local-ack key SECRET_PASSWORD
```

Related Commands

Command	Description
ip slb serverfarm	Identifies a server farm and enters server farm configuration mode.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

radius inject acct key

To configure a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and to enable Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation, use the **radius inject acct key** command in SLB virtual server configuration mode. To disable VSA correlation on this virtual server, use the **no** form of this command.

radius inject acct *group-number* **key** [*encrypt*] *secret-string*

no radius inject acct *group-number* **key** *secret-string*

Syntax Description

group-number	VSA correlation group number to be used for VSA correlation in the RADIUS Accounting-Start packets.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded.

Defaults

VSA correlation is disabled on this virtual server.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

This command is valid only for VSA correlation accounting virtual servers.

Examples

The following example configures VSA correlation group 1 and configures plain text secret string SECRET_STRING for VSA correlation:

```
Router(config-slb-vserver)# radius inject acct 1 key 0 SECRET_STRING
```

Related Commands

Command	Description
radius inject auth	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and specifies whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames.
radius inject auth timer	Configures a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
radius inject auth vsa	Buffers vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.

radius inject auth

To configure a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and to specify whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames, use the **radius inject auth** command in SLB virtual server configuration mode. To disable VSA correlation on this virtual server, use the **no** form of this command.

radius inject auth *group-number* {**calling-station-id** | **username**}

no radius inject auth *group-number* {**calling-station-id** | **username**}

Syntax Description

group-number	VSA correlation group number.
calling-station-id	Specifies that IOS SLB is to create VSA correlation entries based on the RADIUS calling station ID attribute in the RADIUS payload when RADIUS Access-Request messages are exchanged.
username	Specifies that IOS SLB is to create VSA correlation entries based on the RADIUS username attribute in the RADIUS payload when RADIUS Access-Request messages are exchanged.

Defaults

VSA correlation is disabled on this virtual server.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

For a given authentication virtual server, you can configure a single **radius inject auth** *group-number* **calling-station-id** command or a single **radius inject auth** *group-number* **username** command, but not both.

This command is valid only for VSA correlation authentication virtual servers.

Examples

The following example configures VSA correlation group 1 and specifies that IOS SLB is to create VSA correlation entries based on the RADIUS calling station ID attribute:

```
Router(config-slb-vserver)# radius inject auth 1 calling-station-id
```

Related Commands

Command	Description
calling-station-id	Configures an ASCII regular expression string to be matched against the calling station ID attribute in the RADIUS payload.

Command	Description
radius inject acct key	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and enables Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation.
radius inject auth timer	Configures a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
radius inject auth vsa	Buffers vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.
username	Configures an ASCII regular expression string to be matched against the username attribute in the RADIUS payload.

radius inject auth timer

To configure a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, use the **radius inject auth timer** command in SLB virtual server configuration mode. To delete the VSA correlation timer from the configuration, use the **no** form of this command.

radius inject auth timer *seconds*

no radius inject auth timer

Syntax Description

seconds	Time, in seconds, that IOS SLB maintains an entry in the VSA correlation database. Valid range is 1 to 255.

Defaults

No VSA correlation timer is configured for the authentication virtual server.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

This command is valid only for VSA correlation authentication virtual servers.

Examples

The following example configures a VSA correlation timer of 45 seconds:

```
Router(config-slb-vserver)# radius inject auth timer 45
```

Related Commands

Command	Description
radius inject acct key	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and enables Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation.
radius inject auth	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and specifies whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames.
radius inject auth vsa	Buffers vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.

radius inject auth vsa

To buffer vendor-specific attributes (VSAs) for VSA correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, use the **radius inject auth vsa** command in SLB virtual server configuration mode.

radius inject auth vsa *vendor-id*

Syntax Description

vendor-id	VSA to be buffered: • **cisco**—Only the Cisco VSA can be buffered at this time.

Defaults

VSAs are not buffered.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

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

Usage Guidelines

This command is valid only for VSA correlation authentication virtual servers.

Examples

The following example buffers the Cisco VSA:

```
Router(config-slb-vserver)# radius inject auth vsa cisco
```

Related Commands

Command	Description
radius inject acct key	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding accounting virtual server, and enables Message Digest Algorithm Version 5 (MD5) authentication for VSA correlation.
radius inject auth	Configures a vendor-specific attribute (VSA) correlation group for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server, and specifies whether IOS SLB is to create VSA correlation entries based on RADIUS calling station IDs or RADIUS usernames.
radius inject auth timer	Configures a timer for vendor-specific attribute (VSA) correlation for an IOS SLB RADIUS load balancing accelerated data plane forwarding authentication virtual server.

rate

To specify the maximum number of connections allowed for a real server in a server farm, use the **rate** command in real server configuration mode. To remove the rate limit, use the **no** form of this command.

rate *maximum-rate* [**burst** *burst-rate*]

no rate

Syntax Description

maximum-rate	Maximum number of connections allowed for the real server. Valid values range from 1 to 4294967295.
burst *burst-rate*	(Optional) Maximum connection burst rate allowed for the real server. Configure a burst rate if you expect the real server to receive connection requests at random intervals. Valid values range from (*maximum-rate*/10) + 1 to *maximum-rate*. The default burst rate is (*maximum-rate*/10) connections per second. We recommend that you specify a burst rate of at least (*maximum-rate*/4). For example, if *maximum-rate* is set to 3212, the valid range is 322 to 3212; the default burst rate is (3212/10), or 321 connections per second; and we recommend a burst rate of at least (3212/4), or 803 connections per second.

Defaults

There is no limit on the number of connection allowed for the real server.
If you do not configure a burst rate, the default burst rate is (*maximum-rate*/10) connections per second.

Command Modes

Real server configuration (config-slb-real)

Command History

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

Usage Guidelines

The **rate** command is valid only for real servers in server farms. It is not valid for real servers in firewall farms.

If the rate limit for a real server is exceeded, and a new connection request is received, IOS SLB assigns the new connection request to the next **rate**-configured real server in the server farm's queue. If no other **rate**-configured real server is available in the server farm, IOS SLB drops the connection request.

The rate limit also applies to sticky connections. That is, if the rate limit for a real server is exceeded, and a new sticky connection request is received, IOS SLB drops the sticky connection request.

IOS SLB uses slow start even if a real server has a rate limit configured.

Examples

The following example specifies that up to 100 connections per second are allowed for the real server in a server farm, with a burst rate of 25 burst connections per second:

```
Router(config-slb-real)# rate 100 burst 25
```

real (firewall farm)

To identify a firewall as a member of a firewall farm and enter real server configuration mode, use the **real** command in firewall farm configuration mode. To remove the firewall from the IOS Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

real *ip-address*

no real *ip-address*

Syntax Description

ip-address	Real server IP address.

Defaults

No firewall is identified as a member of a firewall farm.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A firewall farm comprises a number of firewalls. The firewalls are the physical devices that provide the firewall load-balanced services.

Examples

The following example identifies a firewall as a member of firewall farm FIRE1:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# real 10.1.1.1
```

Related Commands

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

real (server farm)

To identify a real server as a member of a server farm and enter real server configuration mode, use the **real** command in SLB server farm configuration mode. To remove the real server from the IOS Server Load Balancing (IOS SLB) configuration, use the **no** form of this command.

real *ipv4-address* [**ipv6** *ipv6-address*] [*port*]

no real *ipv4-address* [**ipv6** *ipv6-address*] [*port*]

Syntax Description

ipv4-address	Real server IPv4 address.
ipv6 *ipv6-address*	(Optional) For dual-stack, real server IPv6 address.
port	(Optional) Port translation for the server. Valid values range from 1 to 65535.

Command Default

No real server is identified as a member of a server farm.

Command Modes

SLB server farm configuration (config-slb-sfarm)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(2)E	The *port* argument was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)S	The **ipv6** keyword and *ipv6-address* argument were added.

Usage Guidelines

A server farm comprises a number of real servers. The real servers are the physical devices that provide the load-balanced services.

In general packet radio service (GPRS) load balancing, this command identifies a gateway GPRS support node (GGSN) that is a member of the server farm. Also, remember that the Cisco GGSN IP addresses are virtual template IP addresses, not real interface IP addresses.

IOS SLB supports GPRS Tunneling Protocol (GTP) v0, v1, and v2 real servers. A GTP v2 real server can be either a Packet Data Network Gateway (PGW) or a serving gateway (SGW).

- A GTP v2 PGW can also manage GTP v0 and v1 requests.
- A GTP v2 SGW cannot manage GTP v0 or v1 requests.
- A GTP v0 or v1 real server cannot manage GTP v2 requests. Therefore, you must configure separate virtual servers for GTPv2 real servers and GTP v0 or v1 real servers.

IOS SLB supports dual-stack addresses for GTP load balancing only. To support dual-stack addresses, you must configure the real server as a dual-stack real server, with the IPv4 and IPv6 addresses, using this command.

In Virtual Private Network (VPN) server load balancing, this command identifies a real server acting as a VPN terminator.

Examples

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

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.1.1.1
```

The following example identifies a dual-stack real server as a member of the server farm:

```
Router(config)# ip slb serverfarm DUAL-PUBLIC
Router(config-slb-sfarm)# real 10.1.1.1 ipv6 12AB:0000:0000:CD31:0000:0000:0000:0000/64
```

Related Commands

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

real (static NAT)

To configure one or more real servers to use static Network Address Translation (NAT), use the **real** command in static NAT configuration mode. To restore the default behavior, use the **no** form of this command.

real *ip-address* [*port*]

no real *ip-address* [*port*]

Syntax Description

ip-address	IP address of the real server that is to use static NAT.
port	(Optional) Layer 4 source port number, used by IOS Server Load Balancing (IOS SLB) to differentiate between User Datagram Protocol (UDP) responses from the real server and connections initiated by the real server.

Defaults

No real server is configured to use static NAT.

Command Modes

Static NAT configuration (config-slb-static)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If no port number is specified, IOS SLB uses static NAT for all packets outbound from the real server.

Examples

The following example configures real server 10.1.1.3 to use static NAT:

```
Router(config)# ip slb static nat
Router(config-slb-static)# real 10.1.1.3
```

Related Commands

Command	Description
ip slb static	Configures a real server's NAT behavior and enters static NAT configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb static	Displays information about the static NAT configuration.

reassign

To specify the threshold of consecutive unacknowledged SYNchronize sequence numbers (SYNs) or Create Packet Data Protocol (PDP) requests that, if exceeded, result in an attempted connection to a different real server, use the **reassign** command in SLB real server configuration mode. To restore the default reassignment threshold, use the **no** form of this command.

reassign *threshold*

no reassign

Syntax Description

threshold	Number of unacknowledged TCP SYNs (or Create PDP requests, in general packet radio service [GPRS] load balancing) that are directed to a real server before the connection is reassigned to a different real server. An unacknowledged SYN is one for which no SYN or ACKnowledgment (ACK) is detected before the next SYN arrives from the client. IOS Server Load Balancing (IOS SLB) allows 30 seconds for the connection to be established or for a new SYN to be received. If neither of these occurs within that time, the connection is removed from the IOS SLB database. The 30-second timer is restarted for each SYN as long as the number of connection reassignments specified in the **faildetect numconns (real server)** command is not exceeded. See the **faildetect numconns (real server)** command for more information. Valid threshold values range from one 1 to 4. The default value is 3.

Defaults

The default threshold value is 3.

Command Modes

SLB real server configuration (config-slb-real)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(9)E	This command was modified to support general packet radio service (GPRS) load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Cisco 7600 series routers that are configured with a Supervisor Engine 720.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

IOS SLB does not reassign sticky connections if either of the following conditions is true:

- The real server is not OPERATIONAL or MAXCONNS_THROTTLED.
- The connection is the first for this sticky connection.

In GPRS load balancing, this command specifies the number of consecutive unacknowledged Create PDP requests (not TCP SYNs) that are directed to a gateway GPRS support node (GGSN) before the connection is reassigned to a different GGSN. You must specify a reassign threshold less than the N3-REQUESTS counter value of the serving GRPS support node (SGSN).

Examples

The following example shows how to set the threshold of unacknowledged SYNs to 2:

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# reassign 2
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the IOS SLB feature.
real (server farm)	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
show ip slb reals	Displays information about the real servers.
show ip slb serverfarms	Displays information about the server farm configuration.

replicate casa (firewall farm)

To configure a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch, use the **replicate casa** command in firewall farm configuration mode. To remove a this configuration, use the **no** form of this command.

replicate casa *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string* [*timeout*]]

no replicate casa *listen-ip remote-ip port*

Syntax Description

listen-ip	Listening IP address for state exchange messages that are advertised.
remote-ip	Destination IP address for all state exchange signals.
port	TCP or User Datagram Protocol (UDP) port number or port name for all state exchange signals.
interval	(Optional) Maximum replication delivery interval from 1 to 300 seconds. The default value is 10 seconds. **Note** While IOS SLB does accept the *interval* argument, the **replicate interval** command is the preferred means for setting the replication delivery interval. In fact, if you set the replication delivery interval using the *interval* argument, IOS SLB writes it into the configuration as a **replicate interval** command.
password	(Optional) Specifies the password for Message Digest Algorithm Version 5 (MD5) authentication.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
timeout	(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 default interval is 10 seconds.
The default password encryption is 0 (unencrypted).
The default password timeout is 180 seconds.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *timeout* option allows you to change the password without stopping messages between the backup and primary Layer 3 switches. The default value is 180 seconds.

During the timeout, the backup 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 backup sends and receives packets only with the new password.

When setting a new password timeout, remember the following considerations:

- If you are configuring a new backup, set the timeout to 0 (send packets with the new password immediately). This configuration prevents password mismatches between the new backup and its primary.
- If you are changing the password for an existing backup, set a longer timeout to allow enough time for you to update the password on the primary before the timeout expires. Setting a longer timeout also prevents mismatches between the backup and primary.

If you configure this command but you do not specify the **7** keyword, the secret-string is stored in the plain text.

Examples

The following example configures a stateful backup Layer-3 switch with a listening IP address of 10.10.10.11 and a remote IP address of 10.10.11.12 over HTTP port 4231:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231
```

Related Commands

Command	Description
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb replicate	Displays the configuration of IO SLB IP replication.

replicate casa (virtual server)

To configure a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch, use the **replicate casa** command in virtual server configuration mode. To remove this configuration, use the **no** form of this command.

replicate casa *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string* [*timeout*]]

no replicate casa *listen-ip remote-ip port*

Syntax Description

listen-ip	Listening IP address for state exchange messages that are advertised.
remote-ip	Destination IP address for all state exchange signals.
port	TCP or User Datagram Protocol (UDP) port number or port name for all state exchange signals.
interval	(Optional) Maximum replication delivery interval from 1 to 300 seconds. The default value is 10 seconds. **Note** While IOS SLB does accept the *interval* argument, the **replicate interval** command is the preferred means for setting the replication delivery interval. In fact, if you set the replication delivery interval using the *interval* argument, IOS SLB writes it into the configuration as a **replicate interval** command.
password	(Optional) Specifies the password for Message Digest Algorithm Version 5 (MD5) authentication.
encrypt	(Optional) Indicates how the *secret-string* is represented when the configuration is displayed (for example, **show run**), or how it is written to nonvolatile memory (for example, **write memory**). The possible values are **0** and **7**: • **0**—The *secret-string* is stored in plain text. This is the default setting. • **7**—The *secret-string* is encrypted before it is displayed or written to nonvolatile memory. **Note** If your router is configured to encrypt all passwords, then the password is represented as 7 followed by the encrypted text. See the Cisco IOS **service** command for more details.
secret-string	(Optional) 1- to 64-character clear password value for MD5 authentication. All characters are valid; case is significant. This password must match the password configured on the host agent. The *secret-string* is always sent in plain text when the configuration is downloaded. The *secret-string* must match the secret that is specified on the RADIUS client (for example, the gateway general packet radio service [GPRS] support node [GGSN]).
timeout	(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 default interval is 10 seconds.
The default password encryption is 0 (unencrypted).
The default password timeout is 180 seconds.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.1(3a)E	The **0** and **7** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *timeout* option allows you to change the password without stopping messages between the backup and primary Layer 3 switches. The default value is 180 seconds.

During the timeout, the backup 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 backup sends and receives packets only with the new password.

When setting a new password timeout, remember the following considerations:

- If you are configuring a new backup, set the timeout to 0 (send packets with the new password immediately). This configuration prevents password mismatches between the new backup and its primary.
- If you are changing the password for an existing backup, set a longer timeout to allow enough time for you to update the password on the primary before the timeout expires. Setting a longer timeout also prevents mismatches between the backup and primary.

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate casa** command in virtual server configuration mode.

The Home Agent Director does not support the **replicate casa** command in virtual server configuration mode.

If you configure this command but you do not specify the **7** keyword, the secret-string is stored in the plain text.

Examples

The following example configures a stateful backup Layer-3 switch with a listening IP address of 10.10.10.11 and a remote IP address of 10.10.11.12 over HTTP port 4231:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# replicate casa 10.10.10.11 10.10.11.12 4231
```

Related Commands

Command	Description
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb vserver	Displays information about the virtual servers defined to IOS SLB.

replicate interval (firewall farm)

To set the replication delivery interval for an IOS Server Load Balancing (IOS SLB) firewall farm, use the **replicate interval** command in firewall farm configuration mode. To restore the default interval, use the **no** form of this command.

replicate interval *interval*

no replicate interval

Syntax Description

interval	Maximum replication delivery interval, in seconds. Replication updates are sent to the peer device (CASA or slave) when the interval expires, or when the send buffer (1500 bytes) is full. The valid range is 1 to 300 seconds. The default value is 10 seconds.

Defaults

The default interval is 10 seconds.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate interval** command in firewall farm configuration mode.

The Home Agent Director does not support the **replicate interval** command in firewall farm configuration mode.

Examples

The following example configures a replication interval of 20 seconds:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# replicate interval 20
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS Server Load Balancing (IOS SLB) slave replication.
replicate casa (firewall farm)	Configures a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch
replicate slave (firewall farm)	Enables stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) firewall farm.
show ip slb replicate	Displays the configuration of IOS Server Load Balancing (IOS SLB) IP replication.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

replicate interval (virtual server)

To set the replication delivery interval for an IOS Server Load Balancing (IOS SLB) virtual server, use the **replicate interval** command in virtual server configuration mode. To restore the default interval, use the **no** form of this command.

replicate interval *interval*

no replicate interval

Syntax Description

interval	Maximum replication delivery interval, in seconds. Replication updates are sent to the peer device (CASA or slave) when the interval expires, or when the send buffer (1500 bytes) is full. The valid range is 1 to 300 seconds. The default value is 10 seconds.

Defaults

The default interval is 10 seconds.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate interval** command in virtual server configuration mode.

The Home Agent Director does not support the **replicate interval** command in virtual server configuration mode.

Examples

The following example configures a replication interval of 20 seconds:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# replicate interval 20
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS Server Load Balancing (IOS SLB) slave replication.
replicate casa (virtual server)	Configures a stateful backup of IOS Server Load Balancing (IOS SLB) decision tables to a backup switch
replicate slave (virtual server)	Enables stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) virtual server.
show ip slb replicate	Displays the configuration of IOS Server Load Balancing (IOS SLB) IP replication.
show ip slb vserver	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

replicate slave (firewall farm)

To enable stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) firewall farm, if the slave device is present, use the **replicate slave** command in firewall farm configuration mode. To disable stateful backup of redundant route processors, use the **no** form of this command.

replicate slave

no replicate slave

Syntax Description

This command has no arguments or keywords.

Defaults

Stateful backup of redundant route processors is disabled.

Command Modes

Firewall farm configuration (config-slb-fw)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate slave** command in firewall farm configuration mode.

The Home Agent Director does not support the **replicate slave** command in firewall farm configuration mode.

Examples

The following example enables stateful backup of redundant route processors:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# replicate slave
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS SLB slave replication.
replicate casa (firewall farm)	Configures a stateful backup of IOS SLB decision tables to a backup switch
replicate interval (firewall farm)	Sets the replication delivery interval for an IOS SLB firewall farm.
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

replicate slave (virtual server)

To enable stateful backup of redundant route processors for an IOS Server Load Balancing (IOS SLB) virtual server, if the slave device is present, use the **replicate slave** command in virtual server configuration mode. To disable stateful backup of redundant route processors, use the **no** form of this command.

replicate slave

no replicate slave

Syntax Description

This command has no arguments or keywords.

Defaults

Stateful backup of redundant route processors is disabled.

Command Modes

Virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.2(14)ZA5	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

General packet radio service (GPRS) load balancing without GPRS Tunneling Protocol (GTP) cause code inspection enabled does not support the **replicate slave** command in virtual server configuration mode.

The Home Agent Director does not support the **replicate slave** command in virtual server configuration mode.

If you are using a single Supervisor with **replicate slave** configured, you might receive out-of-sync messages on the Supervisor.

Examples

The following example enables stateful backup of redundant route processors:

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# replicate slave
```

Related Commands

Command	Description
ip slb replicate slave rate	Sets the replication message rate for IOS SLB slave replication.
replicate casa (virtual server)	Configures a stateful backup of IOS SLB decision tables to a backup switch

Command	Description
replicate interval (virtual server)	Sets the replication delivery interval for an IOS SLB virtual server.
show ip slb replicate	Displays the configuration of IOS SLB IP replication.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.

request (custom UDP probe)

To define the payload of the User Datagram Protocol (UDP) request packet to be sent by a custom UDP probe, use the **request** command in custom UDP probe configuration mode.

request data {*start-byte* | **continue**} *hex-data-string*

Syntax Description

data *start-byte*	Identifies the payload offset at which the *hex-data-string* is to be placed into the packet.
data continue	String of characters represented by the *hex-data-string* argument is to be placed after the last defined byte in the request packet.
hex-data-string	Payload of the UDP request packet, up to 100 bytes of data in hexadecimal format.

Defaults

The payload of the UDP request packet is not defined.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter more than one **request** command, to specify the entire UDP payload.

Examples

The following example generates custom UDP probe PROBE6, with the specified 119-byte UDP payload.

```
Router(config)# ip slb probe PROBE6 custom UDP
Router(config-slb-probe)# request data 0 05 04 00 77 18 2A D6 CD 0A AD 53 4D F1 29 29 CF
C1 96 59 CB
Router(config-slb-probe)# request data 20 01 07 63 68 72 69 73 28 06 00 00 00 01 2C 0A 30
30 30 30 30
Router(config-slb-probe)# request data 40 30 30 42 07 06 00 00 00 07 1E 10 63 75 66 66 2E
63 69 73 63
Router(config-slb-probe)# request data 60 6F 2E 63 6F 6D 1F 0C 39 31 39 33 39 32 39 31 36
39 08 06 0A
Router(config-slb-probe)# request data 80 0A 01 01 2D 06 00 00 00 01 3D 06 00 00 00 05 05
06 00 00 00
Router(config-slb-probe)# request data 100 00 06 06 00 00 00 02 04 06 0A 0A 18 0A 29 06 00
00 00 00
```

Related Commands

Command	Description
ip slb probe custom udp	Configures the IOS SLB IP probe name.
response	Defines the data string to match against custom UDP probe response packets.
show ip slb probe	Displays information about an IOS SLB probe.

request (HTTP probe)

To configure an HTTP probe to check the status of the real servers, use the **request** command in HTTP probe configuration mode. To remove a **request** configuration, use the **no** form of this command.

request [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*]

no request [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*]

Syntax Description

method	(Optional) Configures the way the data is requested from the server.
get	Configures the Get method to request data from the server.
post	Configures the Post method to request data from the server.
head	Configures the header data type to request data from the server.
name *name*	Configures the name string of the data to send to the servers to request data. The character string is limited to 15 characters.
url *path*	(Optional) Configures the path from the server.

Defaults

No HTTP probe is configured to check the status of the real servers.

Command Modes

HTTP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **request** command configures the Cisco IOS Server Load Balancing (Cisco IOS SLB) HTTP probe method used to receive data from the server. Only one Cisco IOS SLB HTTP probe can be configured for each server farm.

If no values are configured following the **method** keyword, the default is Get.

If no URL path is set to the server, the default is /.

Examples

The following example configures an IOS SLB HTTP probe named PROBE2, enters HTTP probe configuration mode, and configures HTTP requests to use the post method and the URL /probe.cgi?all:

```
Router(config)# ip slb probe PROBE2 http
Router(config-slb-probe)# request method post url /probe.cgi?all
```

Related Commands

Command	Description
ip slb probe http	Configures the Cisco IOS SLB IP probe name.
show ip slb probe	Displays information about an Cisco IOS SLB probe.

response

To define the data string to match against custom User Datagram Protocol (UDP) probe response packets, use the **response** command in custom UDP probe configuration mode.

response *clause-number* **data** *start-byte hex-data-string*

Syntax Description

clause-number	Identifies the response clause that is being modified. Up to 8 response clauses can be specified, on individual **response** commands.
data *start-byte*	Byte in the UDP response packet at which the *hex-data-string* is to be matched.
hex-data-string	Up to 100 bytes of data, in hexadecimal format, that is to be matched against the UDP response packet payload. If the data does not match, the probe fails.

Defaults

The data string to match against custom UDP probe response packets is not defined.

Command Modes

Custom UDP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can enter up to 8 individual response commands, to parse up to 8 non-contiguous bytes of data.

Examples

In the following example, if the 26th and 27th bytes of the response from *PROBE6* are not *FF FF*, and the 44th and 45th bytes are not *DD DD*, the probe fails.

```
Router(config)# ip slb probe PROBE6 custom UDP
Router(config-slb-probe)# response 1 data 26 FF FF
Router(config-slb-probe)# response 2 data 44 DD DD
```

Related Commands

Command	Description
ip slb probe custom udp	Configures the IOS SLB IP probe name.
request (custom UDP probe)	Defines the payload of the UDP request packet to be sent by a custom UDP probe.
show ip slb probe	Displays information about an IOS SLB probe.

retry (real server)

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

retry *retry-value*

no retry

Syntax Description

retry-value	Time, in seconds, to wait after the detection of a server failure before a new connection to the server is attempted. If the new connection attempt succeeds, the real server is placed in OPERATIONAL state. If the connection attempt fails, the timer is reset, the connection is reassigned, and the process repeats until it is successful or until the server is placed in the OUTOFSERVICE state by the network administrator. Valid values range from 1 to 3600. The default value is 60 seconds. A value of 0 means do not attempt a new connection to the server when it fails.

Defaults

The default retry-value is 60 seconds.

Command Modes

SLB real server configuration (config-slb-real)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

```
Router(config)# ip slb serverfarm PUBLIC
Router(config-slb-sfarm)# real 10.10.1.1
Router(config-slb-real)# retry 120
```

Related Commands

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

sctp

To enter the Stream Control Transmission Protocol (SCTP) configuration, use the **sctp** command in IDSN User Adaptation Layer (IUA) configuration mode. To disable, use the **no** form of this command.

sctp [[**t1-init** *milliseconds*] [**t3-rtx-min** *seconds*] [**t3-rtx-max** *milliseconds*] [**startup-rtx** *number*] [**assoc-rtx** *number*] [**path-rtx** *number*]]

no sctp

Syntax Description

t1-init *milliseconds*	Timer T1 initiation value in milliseconds. Valid values are from 1000 to 60000. The **t1-init** configurable option applies only during the creation of an SCTP instance.
t3-rtx-min *seconds*	Timer T3 retransmission minimum timeout in seconds. Valid values are from 1 to 300.
t3-rtx-max *milliseconds*	Timer T3 retransmission maximum timeout in milliseconds. Valid values are from 1000 to 60000.
startup-rtx *number*	Maximum startup retransmissions. The **startup-rtx** configurable option applies only during the creation of an SCTP instance. Valid values are from 2 to 20.
assoc-rtx *number*	Maximum association retransmissions. Valid values are from 2 to 20.
path-rtx *number*	Maximum path retransmissions. Valid values are from 2 to 20.

Command Default

No default behavior or values.

Command Modes

IUA configuration (config-iua)

Command History

Release	Modification
12.2(15)T	This command was introduced on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

To enter SCTP configuration commands, you must first enter IUA configuration mode and then enter **sctp** at the Router(config-iua)# prompt to enter SCTP configuration mode.

Examples

The following example shows how to enter IUA configuration mode:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# iua
Router(config-iua)#
```

The following is an example of how to set failover time (in milliseconds) between 1 and 10 seconds as part of SCTP configuration of the T1 initiation timer. This example uses the lowest failover timer value allowed (1 second):

```
Router(config-iua)# as as5400-3 fail-over 1000
```

The following is an example of how to set SCTP maximum startup retransmission interval. This example uses the maximum startup retransmission interval value allowed:

```
Router(config-iua)# as as5400-3 sctp-startup 20
```

The following is an example of how to configure the number of SCTP streams for this AS. This example uses the maximum SCTP streams allowed:

```
Router(config-iua)# as as5400-3 sctp-streams 57
```

The following is an example of how to configure the SCTP T1 initiation timer (in milliseconds). This example uses the maximum timer value allowed:

```
Router(config-iua)# as as5400-3 sctp-t1init 60000
```

Related Commands

Command	Description
pri-group (pri-slt)	Specifies an ISDN PRI on a channelized T1 or E1 controller.

serverfarm

To associate an IPv4 server farm with a virtual server, and optionally configure an IPv4 backup server farm, an IPv6 server farm and backup server farm, and specify that sticky connections are to be used in the IPv4 backup server farm, 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 *primary-farm* [**backup** *backup-farm* [**sticky**]]
[**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id*
priority *priority*]

no serverfarm *primary-farm* [**backup** *backup-farm* [**sticky**]]
[**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id*
priority *priority*]

Syntax Description

primary-farm	Name of a primary server farm that has already been defined using the **ip slb serverfarm** command. • For IPv4 or dual-stack, name of the IPv4 server farm. • For IPv6, name of the IPv6 server farm.
backup *backup-farm*	(Optional) Name of a backup server farm that has already been defined using the **ip slb serverfarm** command. • For IPv4 or dual-stack backup, name of the IPv4 server farm. • For IPv6 backup, name of the IPv6 server farm.
sticky	(Optional) Specifies that sticky connections are to be used in the backup server farm.
ipv6-primary *ipv6-primary-farm*	(Optional) For dual-stack, name of the primary IPv6 server farm that has already been defined using the **ip slb serverfarm** command.
ipv6-backup *ipv6-backup-farm*	(Optional) For dual-stack, name of the backup IPv6 server farm that has already been defined using the **ip slb serverfarm** command.

map *map-id* **priority** *priority*	(Optional) Associates an IOS SLB GPRS Tunneling Protocol (GTP) or RADIUS map with the server farm for general packet radio service (GPRS) or RADIUS load balancing. The map ID identifies a specific map that has already been defined using the **ip slb map** command. The priority specifies the order of preference of the specified map. A lower number indicates a higher priority. The range of priorities is 1 to 255. Priorities for different maps do not have to be contiguous. That is, you can have three maps with priorities 1, 5, and 10, respectively. When IOS SLB searches for a match, it does so on the basis of both the map ID and the map priority. Each map ID and each map priority must be unique across all server farms associated with the virtual server. That is, you cannot configure more than one map with the same ID or priority.

Command Default

No real server farm is associated with a virtual server.
If **backup** *backup-farm* is not specified, no IPv4 backup server farm is configured.
If **backup** *backup-farm* is specified but the **sticky** keyword is not specified, sticky connections are not used in the IPv4 backup server farm.
If **ipv6-primary** *ipv6-primary-farm* is not specified, no dual-stack backup server farm is configured.
If **ipv6-backup** *ipv6-backup-farm* is not specified, no dual-stack backup server farm is configured.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(8a)E	The **backup** and **sticky** keywords and the *backup-farm* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRB	The **map** and **priority** keywords and the *map-id* and *priority* arguments were added.
15.0(1)S	The **ipv6-primary** and **ipv6-backup** keywords and the *ipv6-primary-farm* and *ipv6-backup-farm* arguments were added.

Usage Guidelines

RADIUS load balancing and the Home Agent Director do not support the **sticky** keyword.

You can associate more than one server farm with a given virtual server by configuring more than one **serverfarm** command, each with a unique map ID and a unique priority. (That is, each map ID and each map priority must be unique across all server farms associated with the virtual server.)

For GPRS load balancing, if a real server is defined in two or more server farms, each server farm must be associated with a different virtual server.

IOS SLB supports dual-stack addresses for GTP load balancing only.

All IPv4 or IPv6 server farms that are associated with the same virtual server must have the same NAT configuration.

If you associate a primary server farm with a backup server farm, then all of the server farm maps that use that primary server farm must also be configured to use that same backup serverfarm. You cannot configure a server farm map that uses that primary server farm and no backup server farm.

- For example, if you configure primary server farm SF1 with backup server farm SF2, then all of the server farm maps that are configured with SF1 as the primary serverfarm must also be configured with SF2 as the backup serverfarm, as follows:

```
ip slb vserver RADIUS
 virtual 2.2.2.2 udp 0 service radius
 serverfarm SF1 backup SF2 map 1 priority 1
 serverfarm SF1 backup SF2
 inservice
```

- Furthermore, if you configure primary server farm SF1 with backup server farm SF2, you cannot then configure a server farm map to use SF1 as the primary server farm with no backup server farm. That is, the following is not allowed:

```
ip slb vserver RADIUS
 virtual 2.2.2.2 udp 0 service radius
 serverfarm SF1 map 1 priority 1
 serverfarm SF1 backup SF2
 inservice
```

- The backup server farm associated with an IOS SLB protocol map cannot be associated as a backup server farm with any other map in a given virtual server.

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.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.1 tcp www
Router(config-slb-vserver)# serverfarm PUBLIC
```

Related Commands

Command	Description
ip slb serverfarm	Identifies a server farm and enters server farm configuration mode.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).
virtual	Configures the virtual server attributes.

service-module ip redundancy

To link the primary HSRP interface status to that of the satellite interface, use the **service-module ip redundancy** command in satellite interface configuration mode. To remove the link between the primary HSRP interface status and the satellite interface status, use the **no** form of this command.

service-module ip redundancy *group-name*

no service-module ip redundancy *group-name*

Syntax Description

group-name	Name of the hot standby group. This name must match the hot standby group name configured for the primary HSRP interface, which is typically an Ethernet interface.

Defaults

HSRP is disabled.

Command Modes

Satellite interface configuration (config-if)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **service-module ip redundancy** command only when you have two Cisco IP VSAT satellite WAN network modules (NM-1VSAT-GILAT) on separate HSRP-redundant routers that connect to the same outdoor unit (ODU).

This command enables the satellite interface to spoof the line protocol UP state.

Examples

The following example shows how to link the primary HSRP interface status to that of the satellite interface:

```
service-module ip redundancy grp-hsrp
```

Related Commands

Command	Description
standby ip	Activates HSRP.
standby name	Configures the name of the hot standby group.

Command	Description
standby preempt	Enables preemption on the router and optionally configures a preemption delay.
standby track	Configures an interface so that the hot standby priority changes based on the availability of other interfaces.

show debugging

To display information about the types of debugging that are enabled for your router, use the **show debugging** command in privileged EXEC mode.

show debugging

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.3(7)T	The output of this command was enhanced to show TCP Explicit Congestion Notification (ECN) configuration.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The output of this command was enhanced to show the user-group debugging configuration.

Examples

The following is sample output from the **show debugging** command. In this example, the remote host is not configured or connected.

```
Router# show debugging
!
TCP:
  TCP Packet debugging is on
  TCP ECN debugging is on
!
Router# telnet 10.1.25.234
!
Trying 10.1.25.234 ...
!
00:02:48: 10.1.25.31:11001 <---> 10.1.25.234:23 out ECN-setup SYN
00:02:48: tcp0: O CLOSED 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:02:50: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:50: cwnd from 1460 to 1460, ssthresh from 65535 to 2920
00:02:50: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:02:54: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:02:54: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:02:54: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:03:02: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:02: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
```

```
00:03:02: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23 SYN with ECN disabled
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:18: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:18: tcp0: O SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:20: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:20: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:20: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:24: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:24: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:24: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:32: 10.1.25.31:11001 <---> 10.1.25.234:23 congestion window changes
00:03:32: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:32: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
!Connection timed out; remote host not responding
```

The following is sample output from the **show debugging** command when user-group debugging is configured:

```
Router# show debugging
!
usergroup:
 Usergroup Deletions debugging is on
 Usergroup Additions debugging is on
 Usergroup Database debugging is on
 Usergroup API debugging is on
!
```

The following is sample output from the **show debugging** command when SNAP debugging is configured:

```
Router# show debugging
Persistent variable debugging is currently All


SNAP Server Debugging ON


SNAP Client Debugging ON
Router#
```

Table 3 describes the significant fields in the output.

Table 3 show debugging Field Descriptions

Field	Description
OPTS 4	Bytes of TCP expressed as a number. In this case, the bytes are 4.
ECE	Echo congestion experience.
CWR	Congestion window reduced.
SYN	Synchronize connections—Request to synchronize sequence numbers, used when a TCP connection is being opened.
WIN 4128	Advertised window size, in bytes. In this case, the bytes are 4128.

Table 3 show debugging Field Descriptions (continued)

Field	Description
cwnd	Congestion window (cwnd)—Indicates that the window size has changed.
ssthresh	Slow-start threshold (ssthresh)—Variable used by TCP to determine whether or not to use slow-start or congestion avoidance.
usergroup	Statically defined usergroup to which source IP addresses are associated.

show fm slb counters

To display information about the Feature Manager (FM) IOS Server Load Balancing (IOS SLB) counters, use the **show fm slb counters** command in privileged EXEC mode.

show fm slb counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.

Examples

The following sample output from the **show fm slb counters** command shows counter information for virtual server 10.11.11.11:

```
Router# show fm slb counters
FM SLB Purge Counters:
Global Purges:    0
TCP Purges:       0
UDP Purges:       0
Virtual Purges:   0
Flow Purges:      0

FM SLB Netflow Install Counters
[Slot 6 ] Install Request Sent           3
```

Table 4 describes the fields shown in the display.

Table 4 show fm slb counters Field Descriptions

Field	Description
Global Purges	Number of global purges sent by FM IOS SLB.
TCP Purges	Number of TCP purges sent by FM IOS SLB.
UDP Purges	Number of UDP purges sent by FM IOS SLB.
Virtual Purges	Number of virtual purges sent by FM IOS SLB.
Flow Purges	Number of flow purges sent by FM IOS SLB.
Install Request Sent	Number of install requests sent by IOS SLB.

Related Commands

Command	Description
clear fm slb counters	Clears Feature Manager (FM) IOS Server Load Balancing (IOS SLB) counters.

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

show glbp [**capability** [*interface-type interface-number*]] | [[*interface-type interface-number* [*group-number*] [*state*] [**brief**] [**detail**] [**client-cache** [[**age** *number*] [**forwarder** *number*]] | [**mac-address** *address*] | [**summary**]]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.
group-number	(Optional) GLBP group number in the range from 0 to 1023.
state	(Optional) State of the GLBP router, one of the following: **active**, **disabled**, **init**, **listen**, and **standby**.
brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.
detail	(Optional) Displays all the status of the GLBP router in detailed format. The available status are: **active**, **disabled**, **init**, **listen**, **speak**, and **standby**.
capability	(Optional) Displays the GLBP capability interfaces.
client-cache	(Optional) Displays the GLBP client cache.
age *number*	(Optional) Displays the client-cache age in the range from 0 to 1440.
forwarder *number*	(Optional) Displays the client forwarder in the range from 1 to 4.
mac-address *address*	(Optional) Displays the mac-address of the client.
summary	(Optional) Displays the summary of the GLBP client caches.

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. The **client-cache** keyword was added.
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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was enhanced to display information about GLBP support of Stateful Switchover (SSO) mode.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
12.4(15)T	This command was modified. The **client-cache** keyword was added.
12.4(24)T	This command was modified. The **detail** keyword was added. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SXI1	This command was modified. The **client-cache** keyword was added. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SRE	The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.

Usage Guidelines

Use the **show glbp** command to display information about GLBP groups on a router. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder. The **client-cache** keyword displays the client cache details and the **capability** keyword displays all GLBP-capable interfaces.

Examples

The following is sample output from the **show glbp** 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-string
  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-string
  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 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, string "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.bbd3.bc21 (10.0.0.2) local
```

The following output shows GLBP support for SSO mode on an active RP:

```
Router# show glbp

Ethernet0/0 - Group 1
State is Standby
1 state change, last state change 00:00:20
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.232 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
```

```
Active is 172.24.1.2, priority 100 (expires in 7.472 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
aabb.cc00.0200 (172.24.1.2)
There are 2 forwarders (1 active)
Forwarder 1
State is Listen
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Time to live: 14397.472 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 172.24.1.2 (primary), weighting 100 (expires in 9.540 sec)
Forwarder 2
State is Active
1 state change, last state change 00:00:28
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is local, weighting 100
```

The following output shows GLBP support for SSO mode on a standby RP:

```
RouterRP-standby# show glbp

Ethernet0/0 - Group 1
State is Init (standby RP, peer state is Standby)
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
aabb.cc00.0200 (172.24.1.2)
There are 2 forwarders (0 active)
Forwarder 1
State is Init (standby RP, peer state is Listen)
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Preemption enabled, min delay 30 sec
Active is unknown
Forwarder 2
State is Init (standby RP, peer state is Active)
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is unknown
```

GLBP support for Stateful Switchover (SSO) mode is enabled by default but may be disabled by the **no glbp sso** command. If GLBP support for SSO mode is disabled, the output of the **show glbp** command on the standby RP will display a warning:

```
RouterRP-standby# show glbp

Ethernet0/0 - Group 1
State is Init (GLBP SSO disabled) <------ GLBP SSO is disabled.
```

```
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
There are 2 forwarders (0 active)
Forwarder 1
State is Init (GLBP SSO disabled)
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Preemption enabled, min delay 30 sec
Active is unknown
Forwarder 2
State is Init (GLBP SSO disabled)
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is unknown
```

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	State of the virtual gateway or virtual forwarder. For a virtual gateway, the state can be one of the following: • Active—The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled—The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial—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. • Listen—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. • Speak—The virtual gateway is attempting to become the active or standby virtual gateway. • Standby—The gateway is next in line to be the AVG.

Table 5 show glbp Field Descriptions (continued)

Field	Description
	For a virtual forwarder, the state can be one of the following: • Active—The gateway is the active virtual forwarder (AVF) and is responsible for forwarding packets sent to the virtual forwarder MAC address. • 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. • 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. • Listen—The virtual forwarder is receiving hello packets and is ready to change to the "active" state if the AVF becomes unavailable.
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	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. This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.
Active is	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. This field is also displayed under the forwarder section where it indicates the address of the current AVF.
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.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other routers declare the active GLBP router to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

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 [*type number*] **mac**

Syntax Description

type	(Optional) Interface type supported on your router.
number	(Optional) Port number of the interface. The syntax varies depending on the type of 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.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show interface mac** command displays information for one interface, when specified, or all interfaces configured for MAC accounting.

For incoming packets on the interface, the accounting statistics are gathered before the committed access rate (CAR)/distributed committed access rate (DCAR) functionality is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after the CAR output, and before DCAR output or distributed weighted random early detection (DWRED) or distributed weighted fair queuing (DWFQ) functionality is performed on the packet.

Therefore, if DCAR or DWRED is performed on the interface and packets are dropped, the dropped packets are still counted in the **show interface mac** command.

The maximum number of MAC addresses that can be stored for the input and output addresses is 512 each. 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:

```
Router# show interface ethernet 0/1/1 mac

Ethernet0/1/1
  Input  (511 free)
    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
```

Table 6 describes the significant fields shown in the display.

Table 6 show interface mac Field Descriptions

Field	Description
Ethernet0/1/1	Interface type and number.
Input Output	Number of packets received as input or sent as output by this interface.
0007.f618.4449(228)	MAC address of the interface from or to which this router sends or receives packets.
packets	Total number of messages that have been transmitted or received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted or received by the system.
last	Time, in milliseconds, since the last IP packet was transmitted or received on the specified interface.

Related Commands

Command	Description
ip accounting mac-address	Enables IP accounting on any interface based on the source and destination 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

type	(Optional) Interface type supported on your router.
number	(Optional) Port number of the interface. The syntax varies depending on the type of 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
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show interface precedence** command displays information for one interface, when specified, or all interfaces configured for IP precedence accounting.

For incoming packets on the interface, the accounting statistics are gathered before the committed access rate (CAR)/distributed committed access rate (DCAR) functionality is performed on the packet. For outgoing packets on the interface, the accounting statistics are gathered after the CAR output, and before DCAR output or distributed weighted random early detection (DWRED) or distributed weighted fair queuing (DWFQ) functionality is performed on the packet. Therefore, if DCAR or DWRED is performed on the interface and packets are dropped, the dropped packets are still counted in the **show interface mac** command.

To clear the accounting statistics, use the **clear counter** EXEC command.

To configure an interface for IP accounting based on IP precedence, use the **ip accounting precedence** interface configuration command.

Examples

The following is sample output from the **show interface precedence** command. In this example, the total packet and byte counts are calculated for the interface that receives (input) or sends (output) IP packets and sorts the results based on IP precedence.

```
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
```

Table 7 describes the fields shown in the display.

Table 7 show interface precedence Field Descriptions

Field	Description
Ethernet0/1/1	Interface type and number.
Input Output	An interface that receives or sends IP packets and sorts the results based on IP precedence.
Precedence	Precedence value for the specified interface.
packets	Total number of messages that have been transmitted or received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, that have been transmitted or received by the system.

Related Commands

Command	Description
ip accounting precedence	Enables IP accounting on any interface based on IP precedence.

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

checkpoint	(Optional) Indicates that the checkpointed database should be displayed.
output-packets	(Optional) Indicates that information pertaining to packets that passed access control and were routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.
access-violations	(Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** 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 **output-packets** and **access-violations** keywords were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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
 172.16.19.40    192.168.67.20                  7                 306
```

```
172.16.13.55    192.168.67.20                67              2749
172.16.2.50     192.168.33.51                17              1111
172.16.2.50     172.31.2.1                   5               319
172.16.2.50     172.31.1.2                   463             30991
172.16.19.40    172.16.2.1                   4               262
172.16.19.40    172.16.1.2                   28              2552
172.16.20.2     172.16.6.100                 39              2184
172.16.13.55    172.16.1.2                   35              3020
172.16.19.40    192.168.33.51                1986            95091
172.16.2.50     192.168.67.20                233             14908
172.16.13.28    192.168.67.53                390             24817
172.16.13.55    192.168.33.51                214669          9806659
172.16.13.111   172.16.6.23                  27739           1126607
172.16.13.44    192.168.33.51                35412           1523980
192.168.7.21    172.163.1.2                  11              824
172.16.13.28    192.168.33.2                 21              1762
172.16.2.166    192.168.7.130                797             141054
172.16.3.11     192.168.67.53                4               246
192.168.7.21    192.168.33.51                15696           695635
192.168.7.24    192.168.67.20                21              916
172.16.13.111   172.16.10.1                  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
172.16.19.40    192.168.67.20              7          306         77
172.16.13.55    192.168.67.20             67         2749        185
172.16.2.50     192.168.33.51             17         1111        140
172.16.2.50     172.16.2.1                5          319        140
172.16.19.40    172.16.2.1                4          262         77
Accounting data age is 41
```

Table 8 describes the significant fields shown in the displays.

Table 8 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 **access-violations** 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 **access-violations** 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.

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.
ip accounting	Enables IP accounting on an interface.
ip accounting-list	Defines filters to control the hosts for which IP accounting information is kept.
ip accounting-threshold	Sets the maximum number of accounting entries to be created.
ip accounting-transits	Controls the number of transit records that are stored in the IP accounting database.

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 [**daddr** *ip-address* | **detail** | **dport** *destination-port* | **protocol** *protocol-number* | **saddr** *ip-address* | **sport** *source-port*] [**detail** | **internal**]

Syntax Description

daddr *ip-address*	(Optional) Displays the destination address of a given TCP connection. The **detail** keyword displays detailed information about the destination IP address. The **internal** keyword displays internal forwarding agent (FA) information.
detail	(Optional) Displays the detailed statistics.
dport *destination-port*	(Optional) Displays the destination port of a given TCP connection. The **detail** keyword displays detailed information about the destination port. The **internal** keyword displays internal forwarding agent (FA) information.
protocol *protocol-number*	(Optional) Displays the protocol of a given TCP connection. The **detail** keyword displays detailed information about the protocol. The **internal** keyword displays internal forwarding agent (FA) information.
saddr *ip-address*	(Optional) Displays the source address of a given TCP connection. The **detail** keyword displays detailed information about the source IP address. The **internal** keyword displays internal forwarding agent (FA) information.
sport *source-port*	(Optional) Displays the source port of a given TCP connection. The **detail** keyword displays detailed information about the source port. The **internal** keyword displays internal forwarding agent (FA) information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output of the **show ip casa affinities** command:

```
Router# show ip casa affinities

                          Affinity Table
Source Address  Port  Dest Address    Port  Prot
172.16.36.118   1118  172.16.56.13    19    TCP
172.16.56.13    19    172.16.36.118   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
172.44.36.118   1118  172.16.56.13    19    TCP
  Action Details:
    Interest Addr:          172.16.56.19      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
172.16.56.13    19    172.16.36.118   1118  TCP
  Action Details:
    Interest Addr:          172.16.56.19      Interest Port: 1638
    Interest Packet: 0x0104 RST FRAG
    Interest Tickle: 0x0003 FIN SYN
    Dispatch (Layer 2):     NO                Dispatch Address: 10.0.0.0
```

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
forwarding-agent	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.
show ip casa oper	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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip casa oper** command:

```
Router# show ip casa oper

Casa is Active
  Casa control address is 10.10.20.34/32
  Casa multicast address is 239.1.1.1
  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
ip casa oper	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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following 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.

Table 11 show ip casa stats Field Descriptions (continued)

Field	Description
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.
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
show ip casa oper	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**]

Syntax Description

detail	(Optional) Displays detailed statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following 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
10.0.0.0         0.0.0.0         0     172.16.56.2     255.255.255.255  0     ICMP
10.0.0.0         0.0.0.0         0     172.16.56.2     255.255.255.255  0     TCP
10.0.0.0         0.0.0.0         0     172.16.56.13    255.255.255.255  0     ICMP
10.0.0.0         0.0.0.0         0     172.16.56.13    255.255.255.255  0     TCP
172.16.56.2     255.255.255.255  0     10.0.0.0         0.0.0.0         0     TCP
172.16.56.13    255.255.255.255  0     10.0.0.0         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
10.0.0.0         0.0.0.0         0     172.16.56.2     255.255.255.255 0     ICMP
  Service Manager Details:
    Manager Addr:           172.16.56.19      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:          172.16.56.19      Interest Port: 1638
    Interest Packet: 0x8000 ALLPKTS
    Interest Tickle: 0x0107 FIN SYN RST FRAG
    Dispatch (Layer 2):     NO                Dispatch Address: 10.0.0.0
    Advertise Dest Address: YES               Match Fragments:  NO

Source Address  Source Mask     Port  Dest Address    Dest Mask       Port  Prot
10.0.0.0         0.0.0.0         0     172.16.56.2     255.255.255.255 0     TCP
```

```
Service Manager Details:
  Manager Addr:           172.16.56.19      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:          172.16.56.19      Interest Port: 1638
  Interest Packet: 0x8102 SYN FRAG ALLPKTS
  Interest Tickle: 0x0005 FIN RST
  Dispatch (Layer 2):     NO                Dispatch Address: 10.0.0.0
  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.

Table 12 show ip casa wildcard Field Descriptions (continued)

Field	Description
Advertise Dest Address	Destination address.
Match Fragments	Indicates whether the wildcard matches fragments based on Boolean logic.

Related Commands

Command	Description
show ip casa oper	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

agent *subsystem-name*	(Optional) Displays information about the specified DFP agent, such as **slb** for IOS SLB.
detail	(Optional) Displays detailed DFP agent information.

Defaults

If no options are specified, the command displays output for all DFP agents identified by **ip dfp agent** commands, regardless of whether those agents are currently in service (**Inservice: yes**) or active (**AppActive: yes**).

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.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

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 example shows basic information for DFP agent slb:

```
Router# show ip dfp agent slb

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
      ------------------   -------
      172.16.45.27         0
```

The following example shows detailed information for DFP agent slb:

```
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
      ------------------   -------
      172.16.45.27         0

Weight Table Report for Agent SLB

      Weights for Port: 80  Protocol: TCP

          IP Address        Bind ID  Weight
          ---------------   -------  -------
          10.1.1.1           0        65535

      Weights for Port: 0 (wildcard)  Protocol: 0 (wildcard)

          IP Address        Bind ID  Weight
          ---------------   -------  -------
          10.0.0.0           65534    0

Bind ID Table Report for Agent SLB

      Bind IDs for Port: 80  Protocol: TCP

          Bind ID   Client IP        Client Mask
          -------   ---------------  ---------------
          0           10.0.0.0          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 Message Digest Algorithm Version 5 (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	Indicates whether the DFP agent is enabled for communication with a DFP manager.
AppActive	Indicates whether the DFP agent is active.
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.

Table 13 show ip dfp Field Descriptions (continued)

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.

Related Commands

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

show ip helper-address

To display IP address information from the helper-address table, use the **show ip helper-address** command in user EXEC or privileged EXEC mode.

show ip helper-address [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

If no arguments are specified, IP address information for all the entries in the helper-address table is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced in a release earlier than Cisco IOS Release 12.3(2)T.
12.2(33)SRD	This command was integrated into Cisco IOS Release 12.2(33)SRD.
12.2(33)SXI	This command was integrated in a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following is sample output from the **show ip helper-address** command:

```
Router# show ip helper-address

Interface                Helper-Address  VPN VRG Name            VRG State
FastEthernet0/0          172.16.0.0      0   router1             Unknown
Ethernet3/3              172.16.1.0      0   None                Unknown
ATM6/0                   172.16.2.0      0   None                Unknown
Loopback30               172.16.2.1      0   None                Unknown
                         172.16.2.3      0   None                Unknown
                         172.16.5.0      0   None                Unknown
```

Table 14 describes the significant fields shown in the display.

Table 14 show show ip helper-address Field Descriptions

Field	Description
Interface	Name of the interface.
Helper-Address	IP addresses in the helper-address table.

Table 14 show show ip helper-address Field Descriptions (continued)

Field	Description
VPN	Name of the Virtual Private Network (VPN).
VRG Name	Name of the Virtual Router Group (VRG).
VRG State	State of the VRG.

Related Commands

Command	Description
ip helper-address	Enables the forwarding of UDP broadcasts, including BOOTP, received on an interface.

show ip icmp rate-limit

To display all Internet Control Message Protocol (ICMP) unreachable destination messages or unreachable destination messages for a specified interface including the number of dropped packets, use the **show ip icmp rate-limit** command in privileged EXEC mode.

show ip icmp rate-limit [*interface-type interface-number*]

Syntax Description

interface-type	(Optional) Interface type. Type of interface to be configured. **Note** Refer to the **interface** command in the *Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4 for a list of interface types.
interface-number	(Optional) Port, connector, or interface card number. On Cisco 4700 series routers, specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

Defaults

All unreachable statistics for all devices are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following is sample output when the **show ip icmp rate-limit** command is entered and unreachable messages are generated:

```
Router# show ip icmp rate-limit

                          DF bit unreachables        All other unreachables
Interval (millisecond)    500                        500

Interface                 # DF bit unreachables     # All other unreachables
---------                 ---------------------     ------------------------
Ethernet0/0               0                         0
Ethernet0/2               0                         0
Serial3/0/3               0                         19

The greatest number of unreachables on Serial3/0/3 is 19.
```

The following is sample output when the **show ip icmp rate-limit** command is entered and the rate-limit interval has been set at 500. The packet threshold has been set at 1 by using the **ip icmp rate-limit unreachable** command, so the logging will display on the console when the threshold is exceeded. The total suppressed packets since last log message is displayed.

```
Router# show ip icmp rate-limit

00:04:18: %IP-3-ICMPRATELIMIT: 2 unreachables rate-limited within 60000 milliseconds on
Serial3/0/3. 17 log messages suppressed since last log message displayed on Serial3/0/3
```

Table 15 describes the significant fields shown in the display.

Table 15 show ip icmp rate-limit Field Descriptions

Field	Description
ICMPRATELIMIT	ICMP packets that are rate limited.
suppressed	Packets that have been suppressed because the destination is unreachable.

Related Commands

Command	Description
clear icmp rate-limit	Clears all ICMP unreachable destination messages or all messages for a specified interface.
ip icmp rate-limit unreachable	Limits the rate at which ICMP unreachable messages are generated for a destination.

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

Usage Guidelines

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 172.16.80.29

Host              Gateway           Last Use    Total Uses  Interface
172.16.1.111      172.16.80.240        0:00             9  Ethernet0
172.16.1.4        172.16.80.240        0:00             4  Ethernet0
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.
ip mtu	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 sctp association list

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp association list** command is replaced by the **show sctp association list** command. See the **show sctp association list** command for more information.

To display identifiers and information for current Stream Control Transmission Protocol (SCTP) associations and instances, use the **show ip sctp association list** command in privileged EXEC mode.

show ip sctp association list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp association list** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series. Support for the Cisco AS5300 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(11)T	This command was replaced by the **show sctp association list** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

Use this command to display the current SCTP association and instance identifiers, the current state of SCTP associations, and the local and remote port numbers and addresses that are used in the associations.

Examples

The following is sample output from this command for three association identifiers:

```
Router# show ip sctp association list

*** SCTP Association List ****

AssocID:0,  Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8989, Addrs:10.6.0.4 10.5.0.4

AssocID:1,  Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8990, Addrs:10.6.0.4 10.5.0.4

AssocID:2,  Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8991, Addrs:10.6.0.4 10.5.0.4
```

Table 16 describes the significant fields shown in the display.

Table 16 show ip sctp association list Field Descriptions

Field	Description
Assoc ID	SCTP association identifier.
Instance ID	SCTP association instance identifier.
Current state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Local port, Addrs	Port and IP address for the local SCTP endpoint.
Remote port, Addrs	Port and IP address for the remote SCTP endpoint.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show ip sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

show ip sctp association parameters

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp association parameters** command is replaced by the **show sctp association parameters** command. See the **show sctp association parameters** command for more information.

To display configured and calculated parameters for the specified Stream Control Transmission Protocol (SCTP) association, use the **show ip sctp association parameters** command in privileged EXEC mode.

show ip sctp association parameters *assoc-id*

Syntax Description

assoc-id	Association identifier. Shows the associated ID statistics for the SCTP association.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp association parameters** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	Three new output fields were added to this command: Outstanding bytes, per destination address; Round trip time (RTT), per destination address; and Smoothed round trip time (SRTT), per destination address.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.
12.4(11)T	This command was replaced by the **show sctp association parameters** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

The **show ip sctp association parameters** command provides information to determine the stability of SCTP associations, dynamically calculated statistics about destinations, and values to assess network congestion. This command also displays parameter values for the specified association.

This command requires an association identifier. Association identifiers can be obtained from the output of the **show ip sctp association list** command.

Many parameters are defined for each association. Some are configured parameters, and others are calculated. Three main groupings of parameters are displayed by this command:

- Association configuration parameters
- Destination address parameters
- Association boundary parameters

The association configuration section displays information similar to that in the **show ip sctp association list** command, including association identifiers, state, and local and remote port and address information. The current primary destination is also displayed.

Examples

The following sample output shows the IP SCTP association parameters for association 0:

```
Router# show ip sctp association parameters 0

** SCTP Association Parameters **

AssocID: 0  Context: 0  InstanceID: 1
Assoc state: ESTABLISHED  Uptime: 19:05:57.425
Local port: 8181
Local addresses: 10.1.0.3 10.2.0.3

Remote port: 8181
Primary dest addr: 10.5.0.4
Effective primary dest addr: 10.5.0.4
Destination addresses:

10.5.0.4:   State:  ACTIVE
  Heartbeats:  Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/16/38 ms   TOS: 0  MTU: 1500
  cwnd: 5364  ssthresh: 3000  outstand: 768
  Num retrans: 0  Max retrans: 5  Num times failed: 0

10.6.0.4:   State:  ACTIVE
  Heartbeats:  Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/4/7 ms   TOS: 0  MTU: 1500
  cwnd: 3960  ssthresh: 3000  outstand: 0
  Num retrans: 0  Max retrans: 5  Num times failed: 0

Local vertag: 9A245CD4  Remote vertag: 2A08D122
Num inbound streams: 10  outbound streams: 10
Max assoc retrans: 5  Max init retrans: 8
CumSack timeout: 200 ms  Bundle timeout: 100 ms
Min RTO: 1000 ms  Max RTO: 60000 ms
LocalRwnd: 18000  Low: 13455   RemoteRwnd: 15252  Low: 13161
Congest levels: 0  current level: 0  high mark: 325
```

Table 17 describes the significant fields shown in the display.

Table 17 show ip sctp association parameters Field Descriptions

Field	Description
AssocID	SCTP association identifier.
Context	Internal upper-layer handle.
InstanceID	SCTP association instance identifier.

Table 17 show ip sctp association parameters Field Descriptions (continued)

Field	Description
Assoc state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Uptime	How long the association has been active.
Local port	Port number for the local SCTP endpoint.
Local addresses	IP addresses for the local SCTP endpoint.
Remote port	Port number for the remote SCTP endpoint.
Primary dest addr	Primary destination address.
Effective primary dest addr	Current primary destination address.
Heartbeats	Status of heartbeats.
Timeout	Heartbeat timeout.
RTO/RTT/SRTT	Retransmission timeout, round trip time, and smoothed round trip time, calculated from network feedback.
TOS	IP precedence setting.
MTU	Maximum transmission unit size, in bytes, that a particular interface can handle.
cwnd	Congestion window value calculated from network feedback. This value is the maximum amount of data that can be outstanding in the network for that particular destination.
ssthresh	Slow-start threshold value calculated from network feedback.
outstand	Number of outstanding bytes.
Num retrans	Current number of times that data has been retransmitted to that address.
Max retrans	Maximum number of times that data has been retransmitted to that address.
Num times failed	Number of times that the address has been marked as failed.
Local vertag, Remote vertag	Verification tags (vertags). Tags are chosen during association initialization and do not change.
Num inbound streams, Num outbound streams	Maximum inbound and outbound streams. This number does not change.
Max assoc retrans	Maximum association retransmit limit. Number of times that any particular chunk may be retransmitted before a declaration that the association failed, which indicates that the chunk could not be delivered on any address.
Max init retrans	Maximum initial retransmit limit. Number of times that the chunks for initialization may be retransmitted before a declaration that the attempt to establish the association failed.
CumSack timeout	Cumulative selective acknowledge (SACK) timeout. The maximum time that a SACK may be delayed while attempting to bundle together with data chunks.
Bundle timeout	Maximum time that data chunks may be delayed while attempts are made to bundle them with other data chunks.

Table 17 show ip sctp association parameters Field Descriptions (continued)

Field	Description
Min RTO, Max RTO	Minimum and maximum retransmit timeout values allowed for the association.
LocalRwnd, RemoteRwnd	Local and remote receive windows.
Congest levels: current level, high mark	Current congestion level and highest number of packets queued.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays all currently defined SCTP instances.
show ip sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

show ip sctp association statistics

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp association statistics** command is replaced by the **show sctp association statistics** command. See the **show sctp association statistics** command for more information.

To display statistics that have accumulated for the specified Stream Control Transmission Protocol (SCTP) association, use the **show ip sctp association statistics** command in privileged EXEC mode.

show ip sctp association statistics *assoc-id*

Syntax Description

assoc-id	Association identifier, which can be obtained from the output of the **show ip sctp association list** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp association statistics** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	Two new output fields were added to this command: Number of unordered data chunks sent and Number of unordered data chunks received. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(11)T	This command was replaced by the **show sctp association statistics** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command shows only the information that has become available since the last time a **clear ip sctp statistics** command was executed.

Examples

The following sample output shows the statistics accumulated for SCTP association 0:

```
Router# show ip sctp association statistics 0

** SCTP Association Statistics **

AssocID/InstanceID: 0/1
Current State: ESTABLISHED
Control Chunks
  Sent: 623874  Rcvd: 660227
Data Chunks Sent
  Total: 14235644  Retransmitted: 60487
  Ordered: 6369678  Unordered: 6371263
  Avg bundled: 18  Total Bytes: 640603980
Data Chunks Rcvd
  Total: 14496585  Discarded: 1755575
  Ordered: 6369741  Unordered: 6371269
  Avg bundled: 18  Total Bytes: 652346325
  Out of Seq TSN: 3069353
ULP Dgrams
  Sent: 12740941  Ready: 12740961  Rcvd: 12740941
```

Table 18 describes the significant fields shown in the display.

Table 18 show ip sctp association statistics Field Descriptions

Field	Description
AssocID/InstanceID	SCTP association identifier and instance identifier.
Current State	State of SCTP association.
Control Chunks	SCTP control chunks sent and received.
Data Chunks Sent	SCTP data chunks sent, ordered and unordered.
Data Chunks Rcvd	SCTP data chunks received, ordered and unordered.
ULP Dgrams	Number of datagrams sent, ready, and received by the Upper-Layer Protocol (ULP).

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays all currently defined SCTP instances.
show ip sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

show ip sctp errors

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp errors** command is replaced by the **show sctp errors** command. See the **show sctp errors** command for more information.

To display the error counts logged by the Stream Control Transmission Protocol (SCTP), use the **show ip sctp errors** command in privileged EXEC mode.

show ip sctp errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp errors** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(11)T	This command was replaced by the **show sctp errors** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command displays all errors across all associations that have been logged since the last time that the SCTP statistics were cleared with the **clear ip sctp statistics** command. If no errors have been logged, this is indicated in the output.

Examples

The following sample output shows a session with no errors:

```
Router# show ip sctp errors

*** SCTP Error Statistics ****

No SCTP errors logged.
```

The following sample output shows a session that has SCTP errors:

```
Router# show ip sctp errors

** SCTP Error Statistics **

Invalid verification tag:       5
Communication Lost:             64
Destination Address Failed:     3
Unknown INIT params rcvd:       16
Invalid cookie signature:       5
Expired cookie:                 1
Peer restarted:                 1
No Listening instance:          2
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show ip sctp instances

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp instances** command is replaced by the **show sctp instances** command. For more information, see the **show sctp instances** command.

To display information for each of the currently configured Stream Control Transmission Protocol (SCTP) instances, use the **show ip sctp instances** command in privileged EXEC mode.

show ip sctp instances

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp instances** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(11)T	This command was replaced by the **show sctp instances** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command displays information for each of the currently configured instances. The instance number, local port, and address information are displayed. The instance state is either available or deletion pending. An instance enters the deletion pending state when a request is made to delete it but there are currently established associations for that instance. The instance cannot be deleted immediately and instead enters the pending state. No new associations are allowed in this instance, and when the last association is terminated or fails, the instance is deleted.

The default inbound and outbound stream numbers are used for establishing incoming associations, and the maximum number of associations allowed for this instance is shown. Then a snapshot of each existing association is shown, if any exists.

Effective with Cisco IOS Release 12.4(11)T, if you enter the **show ip sctp instances** command, you must type the complete word **instances** in the command syntax.

Examples

The following sample output shows available IP SCTP instances. In this example, two current instances are active and available. The first is using local port 8989, and the second is using 9191. Instance identifier 0 has three current associations, and instance identifier 1 has no current associations.

```
Router# show ip sctp instances

*** SCTP Instances ****

Instance ID:0  Local port:8989
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1
  Current associations: (max allowed:6)
  AssocID:0  State:ESTABLISHED  Remote port:8989
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:1  State:ESTABLISHED  Remote port:8990
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:2  State:ESTABLISHED  Remote port:8991
    Dest addrs:10.6.0.4 10.5.0.4

Instance ID:1  Local port:9191
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1

No current associations established for this instance.
Max allowed:6
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show ip sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show ip sctp statistics

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp statistics** command is replaced by the **show sctp statistics** command. See the **show sctp statistics** command for more information.

To display the overall statistics counts for Stream Control Transmission Protocol (SCTP) activity, use the **show ip sctp statistics** command in privileged EXEC mode.

show ip sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp statistics** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.4(11)T	This command was replaced by the **show sctp statistics** command.
12.4(15)T	This command was moved to the Cisco IP Application Services Command Reference.

Usage Guidelines

This command displays the overall SCTP statistics accumulated since the last **clear ip sctp statistics** command. It includes numbers for all currently established associations, and for any that have been terminated. The statistics indicated are similar to those shown for individual associations.

Examples

The following sample output shows IP SCTP statistics:

```
Router# show ip sctp statistics

*** SCTP Overall Statistics ****

Total Chunks Sent:           2097
Total Chunks Rcvd:           2766

Data Chunks Rcvd In Seq:     538
Data Chunks Rcvd Out of Seq: 0
Total Data Chunks Sent:      538
Total Data Chunks Rcvd:      538
Total Data Bytes Sent:       53800
Total Data Bytes Rcvd:       53800
Total Data Chunks Discarded: 0
Total Data Chunks Retrans:   0

Total SCTP Dgrams Sent:      1561
Total SCTP Dgrams Rcvd:      2228
Total ULP Dgrams Sent:       538
Total ULP Dgrams Ready:      538
Total ULP Dgrams Rcvd:       538
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured and calculated for the association defined by the association identifier.
show ip sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays all currently defined SCTP instances.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show ip slb conns

To display the active IOS Server Load Balancing (IOS SLB) connections (or sessions, in GPRS load balancing and the Home Agent Director), use the **show ip slb conns** command in privileged EXEC mode.

show ip slb conns [**vserver** *virtual-server* | **client** *ip-address* | **firewall** *firewall-farm*] [**detail**]

Syntax Description

vserver *virtual-server*	(Optional) Displays only those connections (or sessions, in GPRS load balancing and the Home Agent Director) associated with the specified virtual server.
client *ip-address*	(Optional) Displays only those connections (or sessions, in GPRS load balancing and the Home Agent Director) associated with the specified client IP address.
firewall *firewall-farm*	(Optional) Displays only those connections (or sessions, in GPRS load balancing and the Home Agent Director) associated with the specified firewall farm.
detail	(Optional) Displays detailed information about the connection (or session, in GPRS load balancing and the Home Agent Director).

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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(7)E	The **firewall** keyword and *firewall-farm* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If no options are specified, the command displays output for all active IOS SLB connections (or sessions, in GPRS load balancing and the Home Agent Director).

Examples

The following is sample output from the **show ip slb conns** command:

```
Router# show ip slb conns

vserver          prot   client               real                 state
---------------------------------------------------------------------------
TEST             TCP    10.150.72.183:328    10.80.90.25:80       INIT
TEST             TCP    10.250.167.226:423   10.80.90.26:80       INIT
TEST             TCP    10.234.60.239:317    10.80.90.26:80       ESTAB
TEST             TCP    10.110.233.96:747     10.80.90.26:80       ESTAB
```

```
TEST            TCP    10.162.0.201:770      10.80.90.30:80        CLOSING
TEST            TCP    10.22.225.219:995     10.80.90.26:80        CLOSING
TEST            TCP    10.2.170.148:169      10.80.90.30:80        ZOMBIE
```

Table 19 describes the fields shown in the display.

Table 19 show ip slb conns Field Descriptions

Field	Description
vserver	Name of the virtual server associated with the connection (or session, in GPRS load balancing and the Home Agent Director).
prot	Protocol being used by the connection (or session, in GPRS load balancing and the Home Agent Director).
client	Client IP address associated with the connection (or session, in GPRS load balancing and the Home Agent Director).
real	Real server IP address associated with the connection (or session, in GPRS load balancing and the Home Agent Director).
state	Current state of the connection (or session, in GPRS load balancing and the Home Agent Director). • CLOSING—The connection is closing. • ESTAB—The connection has been established and is operational. • INIT—The connection is being initialized. • ZOMBIE—The connection is currently pending destruction (awaiting a timeout or some other condition to be met).

show ip slb dfp

To display Dynamic Feedback Protocol (DFP) manager and agent information, such as passwords, timeouts, retry counts, and weights, use the **show ip slb dfp** command in privileged EXEC mode.

show ip slb dfp [**agent** *agent-ip port* | **manager** *manager-ip* | **detail** | **weights**]

Syntax Description

agent	(Optional) Displays information about an agent.
agent-ip	(Optional) Agent IP address.
port	(Optional) Agent TCP or User Datagram Protocol (UDP) port number.
manager	(Optional) Displays information about the specified manager.
manager-ip	(Optional) Manager IP address.
detail	(Optional) Displays all data available.
weights	(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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(5a)E	The **manager** keyword and *manager-ip* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If no options are specified, the command displays summary information.

Examples

The following sample output from the **show ip slb dfp** command displays high-level information about all DFP agents and managers:

```
Router# show ip slb dfp
DFP Manager:
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:0 sec

Agent IP          Port    Timeout   Retry Count   Interval
-------------------------------------------------------------
172.16.2.34       61936   0         0             180 (Default)
```

Table 20 describes the fields shown in the display.

Table 20 show ip slb dfp Field Descriptions

Field	Description
DFP Manager	Indicates that the following information applies to the DFP manager.
Current passwd	Current password for the DFP manager, if any.
Pending passwd	Pending password for the DFP manager, if any.
Passwd timeout	For the DFP manager, delay period, in seconds, during which both the current password and the pending password are accepted.
Agent IP	IP address of the agent about which information is being displayed.
Port	TCP or UDP port number of the agent. The valid range is 1 to 65535.
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.

The following example displays detailed information about DFP agents and managers:

```
Router# show ip slb dfp detail
DFP Manager
      Current passwd <none> Pending passwd <none>
      Passwd timeout 0 sec
      Unexpected errors 0
% No DFP Agents configured
```

Table 21 describes the fields shown in the display.

Table 21 show ip slb dfp detail Field Descriptions

Field	Description
DFP Manager	Indicates that the following information applies to the DFP manager.
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 pending password are accepted.
Unexpected errors	Number of unexpected errors encountered by the DFP manager.
No DFP Agents configured	Indicates that there are no DFP agents associated with the DFP manager.

The following example displays detailed information about DFP manager 10.0.0.0:

```
Router# show ip slb dfp manager 10.0.0.0
DFP Manager 10.0.0.0 Connection state Connected
   Timeout = 20
   Last message sent 033537 UTC 01/02/00
```

Table 22 describes the fields shown in the display.

Table 22 show ip slb dfp manager Field Descriptions

Field	Description
DFP Manager	Indicates that the following information applies to the DFP manager.
Connection state	Current connection state of the DFP manager.
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.
Last message sent	Date and time of the last message sent by the DFP manager.

The following example displays detailed information about weights assigned to real servers for load balancing:

```
Router# show ip slb dfp weights
Real IP Address 10.0.10.10 Protocol TCP Port 22 Bind_ID 111 Weight 111
      Set by Agent 172.16.2.3458490 at 132241 UTC 12/03/99
Real IP Address 10.17.17.17 Protocol TCP Port www Bind_ID 1 Weight 1
      Set by Agent 172.16.2.3458490 at 132241 UTC 12/03/99
Real IP Address 10.68.68.68 Protocol TCP Port www Bind_ID 4 Weight 4
      Set by Agent 172.16.2.3458490 at 132241 UTC 12/03/99
Real IP Address 10.85.85.85 Protocol TCP Port www Bind_ID 5 Weight 5
      Set by Agent 172.16.2.3458490 at 132241 UTC 12/03/99
```

Table 23 describes the fields shown in the display.

Table 23 show ip slb dfp weights Field Descriptions

Field	Description
Real IP Address	IP address of the real server for which weight is reported.
Protocol	Protocol used for the port.
Port	Port for which the following bind ID is being reported.
Bind_ID	Bind ID of this instance of the real server.
Weight	Weight calculated for the real IP address.
Set by Agent	Agent that set the weight, and the date and time the weight was set.

show ip slb firewallfarm

To display firewall farm information, use the **show ip slb firewallfarm** command in privileged EXEC mode.

show ip slb firewallfarm [**detail**]

Syntax Description

detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip slb firewallfarm** command:

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-------------------------------------------------
FIRE1            IPADDR      OPERATIONAL     2
```

Table 24 describes the fields shown in the display.

Table 24 show ip slb firewallfarm Field Descriptions

Field	Description
firewall farm	Name of the firewall farm.
hash	Load-balancing algorithm used to select a firewall for the firewall farm: • IPADDR—Uses the source and destination IP addresses in the algorithm. • IPADDRPORT—Uses the source and destination TCP or User Datagram Protocol (UDP) port numbers, in addition to the source and destination IP addresses, in the algorithm. See the **predictor hash address (firewall farm)** command for more details.

Table 24 show ip slb firewallfarm Field Descriptions (continued)

state	Current state of the firewall farm: • OPERATIONAL—Functioning properly. • OUTOFSERVICE—Removed from the load-balancing predictor lists. • STANDBY—Backup firewall farm, ready to become operational if the active firewall farm fails.
reals	Number of firewalls that are members of the firewall farm.

show ip slb fragments

To display information from the Cisco IOS Server Load Balancing (IOS SLB) fragment database, use the **show ip slb fragments** command in privileged EXEC mode.

show ip slb fragments

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following sample output from the **show ip slb fragments** command shows fragment information for virtual server 10.11.11.11:

```
Router# show ip slb fragments

ip src          id    forward         src nat         dst nat
-----------------------------------------------------------------------
10.11.2.128     12    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     13    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     14    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     15    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     16    10.11.2.128     10.11.11.11     10.11.2.128
```

Table 25 describes the fields shown in the display.

Table 25 show ip slb fragments Field Descriptions

Field	Description
ip src	Source IP address of the fragment.
id	IP ID of the fragment, set by the packet originator.
forward	IP address to which the fragment is being forwarded.
src nat	If using Network Address Translation (NAT), new source IP address after NAT.
dst nat	If using NAT, new destination IP address after NAT.

show ip slb gtp

To display IOS Server Load Balancing (IOS SLB) general packet radio service (GPRS) Tunneling Protocol (GTP) information, use the **show ip slb gtp** command in privileged EXEC mode.

show ip slb gtp {**gsn** [*gsn-ip-address*] | **nsapi** [*nsapi-key*] [**detail**]}

Syntax Description

gsn	(Optional) Displays IOS SLB database information for the specified gateway GPRS support node (GGSN) or serving GPRS support node (SGSN).
gsn-ip-address	(Optional) IP address of the GGSN or SGSN for which information is to be displayed. If you do not specify a *gsn-ip-address*, IOS SLB displays information for all GGSNs and SGSNs.
nsapi	(Optional) Displays IOS SLB database information for the specified Network Service Access Point Identifier (NSAPI).
nsapi-key	(Optional) Key of the NSAPI for which information is to be displayed. If you do not specify an *nsapi-key*, IOS SLB displays information for all NSAPIs.
detail	(Optional) Displays additional, more detailed information.

Defaults

If you specify **gsn** and you do not specify a *gsn-ip-address*, IOS SLB displays information for all GGSNs and SGSNs.
If you specify **nsapi** and you do not specify an *nsapi-key*, IOS SLB displays information for all NSAPIs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(13)E3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip slb gtp gsn** command for a specific GGSN or SGSN:

```
Router# show ip slb gtp gsn 10.0.0.0

type ip              recovery-ie  purging
-----------------------------------------
SGSN 10.0.0.0 UNKNOWN      N
```

Table 26 describes the fields shown in the display.

Table 26 show ip slb gtp gsn Field Descriptions

Field	Description
type	Type of GSN (either GGSN or SGSN).

Table 26 show ip slb gtp gsn Field Descriptions (continued)

ip	IP address of the GGSN or SGSN.
recovery-ie	Last seen recovery IE for this GGSN or SGSN.
purging	Indicates whether Packet Data Protocol (PDP) contexts belonging to this GGSN or SGSN are being purged as a result of path failure: • **Y (Yes)**—PDP contexts are being purged. • **N (No)**—PDP contexts are not being purged.

The following is sample output from the **show ip slb gtp nsapi** command:

```
Router# show ip slb gtp nsapi

nsapi key        real                  nsapi count session count
-----------------------------------------------------------------
11111111111111F1 172.16.0.0 1          1
```

The following is sample output from the **show ip slb gtp nsapi** command for a specific NSAPI key:

```
Router# show ip slb gtp nsapi 11111111111111F1

nsapi key        real                  nsapi count session count
-----------------------------------------------------------------
11111111111111F1 172.16.0.0 1          1
```

Table 27 describes the fields shown in the display.

Table 27 show ip slb gtp nsapi Field Descriptions

Field	Description
nsapi key	Key for the session. This is the IMSI.
real	Real server to which the session is assigned.
nsapi count	Number of NSAPIs bound to the session. This is the number of PDP contexts (mobile sessions) on the GGSN associated with the IMSI.
session count	Number of sessions to which the NSAPI is currently bound. Normally, the NSAPI is bound to one session, but it is bound to two sessions in transition during an update.

The following is sample output from the **show ip slb gtp nsapi detail** command:

```
Router# show ip slb gtp nsapi detail

IMSI key = 11111111111111F1, real = 172.16.0.1, nsapi count = 1, session count = 1
no vserver          key              client                 state      seq
-------------------------------------------------------------------------------
5  SERVER1          0009E8810009E881 10.0.0.0:2123        GTP_INIT   0
```

Table 28 describes the fields shown in the display.

Table 28 show ip slb gtp nsapi detail Field Descriptions

Field	Description
IMSI key	IMSI key for the session.
real	Real server to which the session is assigned.
nsapi count	Number of NSAPIs bound to the session. This is the number of PDP contexts (mobile sessions) on the GGSN associated with this IMSI.
session count	Number of sessions to which the NSAPI is currently bound. Normally, the NSAPI is bound to one session, but it is bound to two sessions in transition during an update.
no	NSAPI number.
vserver	Name of the virtual server.
key	Session key.
client	SGSN IP address and port number.
state	State of the session. Possible states are: • **GTP_ESTAB**—The session has been established successfully. • **GTP_INIT**—The PDP contexts have been deleted as a result of a delete request or a deletion in GGSN, and IOS SLB is waiting to destroy the session after the GTP_TIMEOUT. • **GTPIO_REQ_CLIENT**—Waiting for a response from the real server.
seq	Sequence number in the last delete request.

show ip slb map

To display information about IOS SLB protocol maps, use the **show ip slb map** command in privileged EXEC mode.

show ip slb map [*id*]

Syntax Description

id	(Optional) Displays information about the specified map.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If no ID is specified, the command displays information about all maps.

Examples

The following is sample output from the **show ip slb map** command:

```
Router# show ip slb map
ID: 1, Service: GTP
 APN: Cisco.com, yahoo.com
 PLMN ID(s): 11122, 444353
 SGSN access list: 100
ID: 2, Service: GTP
 PLMN ID(s): 67523, 345222
 PDP Type: IPv4, PPP
ID: 3, Service: GTP
 PDP Type: IPv6
ID: 4, Service: RADIUS
 Calling-station-id: "?919*"
ID: 5, Service: RADIUS
 Username: "..778cisco.*"
```

Table 19 describes the fields shown in the display.

Table 29 show ip slb map Field Descriptions

Field	Description
ID	Identifier of the map about which information is being displayed. Information about each map is displayed on a separate line.
Service	Protocol associated with the map. Valid protocols are: • GTP—For general packet radio service (GPRS) Tunneling Protocol (GTP) maps • RADIUS—For RADIUS load balancing maps
APN	One or more access point names (APNs) associated with the GTP map

Table 29 show ip slb map Field Descriptions (continued)

PLMN ID(s)	One or more public land mobile networks (PLMNs) associated with the GTP map.
SGSN access list	Serving GPRS Support Node (SGSN) access list associated with the GTP map.
PDP Type	One or more packet data protocol (PDP) types associated with the GTP map.
Calling-station-id	String to be matched against the calling station ID attribute in the RADIUS payload.
Username	String to be matched against the username attribute in the RADIUS payload.

show ip slb natpool

To display the IP Cisco IOS Server Load Balancing (IOS SLB) Network Address Translation (NAT) configuration, use the **show ip slb natpool** command in privileged EXEC mode.

show ip slb natpool [**name** *pool*] [**detail**]

Syntax Description

name *pool*	(Optional) Displays the specified NAT pool.
detail	(Optional) Lists all the interval ranges currently allocated in the client NAT pool.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the default **show ip slb natpool** command:

```
Router# show ip slb natpool

nat client B  209.165.200.225 1.1.1.6  1.1.1.8  Netmask 255.255.255.0
nat client A  10.1.1.1  1.1.1.5  Netmask 255.255.255.0
```

The following is sample output from the **show ip slb natpool** command with the **detail** keyword:

```
Router# show ip slb natpool detail

nat client A  1.1.1.1  1.1.1.5  Netmask 255.255.255.0
     Start NAT        Last NAT         Count     ALLOC/FREE
     -----------------------------------------------------
     10.1.1.1:11001    10.1.1.1:16333    0005333   ALLOC
     10.1.1.1:16334    10.1.1.1:19000    0002667   ALLOC
     10.1.1.1:19001    10.1.1.5:65535    0264675   FREE

nat client B  1.1.1.6  1.1.1.8  Netmask 255.255.255.0
     Start NAT        Last NAT         Count     ALLOC/FREE
     -----------------------------------------------------
     10.1.1.6:11001    10.1.1.6:16333    0005333   ALLOC
     10.1.1.6:16334    10.1.1.6:19000    0002667   ALLOC
     10.1.1.6:19001    10.1.1.8:65535    0155605   FREE
```

Table 30 describes the fields shown in the display.

Table 30 show ip slb natpool detail Field Descriptions

Field	Description
Start NAT	Starting NAT address in a range of addresses in the client NAT pool.
Last NAT	Last NAT address in a range of addresses in the client NAT pool.
Count	Number of NAT addresses in the range.
ALLOC/FREE	Indicates whether the range of NAT addresses has been allocated or is free.

Related Commands

Command	Description
ip slb natpool	Configures the IOS SLB NAT.

show ip slb probe

To display information about a Cisco IOS Server Load Balancing (IOS SLB) probe, use the **show ip slb probe** command in privileged EXEC mode.

show ip slb probe [**name** *probe*] [**detail**]

Syntax Description

name *probe*	(Optional) Displays information about the specified probe.
detail	(Optional) Displays detailed information, including the SA Agent operation ID, which you can correlate with the output of the **show rtr operational-state** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip slb probe** command:

```
Router# show ip slb probe

Server:Port             State        Outages  Current  Cumulative
-------------------------------------------------------------------
10.10.4.1:0             OPERATIONAL        0  never    00:00:00
10.10.5.1:0             FAILED             1  00:00:06 00:00:06
```

Table 31 describes the fields shown in the display.

Table 31 show ip slb probe Field Descriptions

Field	Description
Server:Port	IP address and port of the real server.
State	Operational state of the probe: • FAILED—The probe has succeeded in the past but has currently failed. • OPERATIONAL—The probe is functioning normally. • TESTING—The probe has never succeeded, due to no response. IOS SLB keeps no counters or timers for this state. For a detailed listing of real server states, see the **show ip slb reals** command.
Outages	Number of intervals between successful probes.

Table 31 show ip slb probe Field Descriptions (continued)

Current	Time since the last probe success. That is, the duration (so far) of the current outage.
Cumulative	Total time the real server has been under test by the probe and has failed the probe test. This value is the sum of the Current time plus the total time of all previous outages.

show ip slb reals

To display information about the real servers, use the **show ip slb reals** command in privileged EXEC mode.

show ip slb reals [**sfarm** *server-farm*] [**detail**]

Syntax Description

sfarm *server-farm*	(Optional) Displays information about those real servers associated with the specified server farm or firewall farm.
detail	(Optional) Displays detailed 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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(13)E	The **vserver** keyword and *virtual-server* argument were replaced with the **sfarm** keyword and *server-farm* argument.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The output for the **detail** keyword for a real server in a server farm was updated to display the configured maximum number of connections allowed (**rate**).
15.0(1)S	The output for the **detail** keyword for a real server in a server farm was updated to display the real server's IPv4, IPv6, or dual-stack address.

Usage Guidelines

If no options are specified, the command displays information about all real servers.

In a configuration with stateful backup, if a probe changes state at the same time that the primary IOS SLB device fails over to the backup IOS SLB device, the output from the **show ip slb reals** command for the backup device displays the state of the probe before the failover, not the actual current state.

Examples

The following is sample output from the **show ip slb reals** command:

```
Router# show ip slb reals

real             farm name        weight   state           conns
-------------------------------------------------------------------
10.80.2.112      FRAG             8        OUTOFSERVICE    0
10.80.5.232      FRAG             8        OPERATIONAL     0
10.80.15.124     FRAG             8        OUTOFSERVICE    0
10.254.2.2       FRAG             8        OUTOFSERVICE    0
10.80.15.124     LINUX            8        OPERATIONAL     0
```

```
10.80.15.125     LINUX           8        OPERATIONAL     0
10.80.15.126     LINUX           8        OPERATIONAL     0
10.80.90.25      SRE             8        OPERATIONAL     220
10.80.90.26      SRE             8        OPERATIONAL     216
10.80.90.27      SRE             8        OPERATIONAL     216
10.80.90.28      SRE             8        TESTING         1
10.80.90.29      SRE             8        OPERATIONAL     221
10.80.90.30      SRE             8        OPERATIONAL     224
10.80.30.3       TEST            100      READY_TO_TEST   0
10.80.30.4       TEST            100      READY_TO_TEST   0
10.80.30.5       TEST            100      READY_TO_TEST   0
10.80.30.6       TEST            100      READY_TO_TEST   0
```

Table 32 describes the fields shown in the display.

Table 32 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.
farm name	Name of the server farm or firewall farm with which the real server is associated.
weight	Weight assigned to the real server. The weight identifies the real server's capacity, relative to other real servers in the server farm.
state	Current state of the real server. • DFP_THROTTLED—The Dynamic Feedback Protocol (DFP) agent sent a weight of 0 for this real server (send no further connections to this real server). • FAILED—The real server has failed as a result of either no response or reset (RST) responses to client traffic. (See the **faildetect numconns (real server)** command for more information about controlling tolerance for no responses and RSTs.) The real server has been removed from use by the predictor algorithms. The retry timer has started. • MAXCONNS_THROTTLE—The number of connections on the real server exceeds the configured maximum number of simultaneous active connections (**maxconns**). • OPERATIONAL—The real server is functioning properly and is being used for load-balancing. • OPER_WAIT—The real server is waiting to become operational (waiting for a timeout or some other condition to be met). • OUTOFSERVICE—The real server was configured with **no inservice** and has been removed from the load-balancing predictor lists. • PROBE_FAILED—The probe has succeeded in the past but has currently failed. This failure might occur at the same time user connections fail, or it might not. • PROBE_TESTING—The probe has never succeeded, due to no response. The initial probe timed out waiting for a success.

Table 32 show ip slb reals Field Descriptions (continued)

	• READY_TO_TEST—The real server is queued for testing after being in FAILED state until the retry timer expired. • TESTING—The real server is queued for assignment. When a single user connection is assigned to a real server that is in READY_TO_TEST state, the real server is placed in TESTING state. If the test succeeds, the real server is placed back in OPERATIONAL state. • TEST_WAIT—The real server is waiting to begin testing (waiting for a timeout or some other condition to be met).
conns	Number of connections associated with the real server. In general packet radio service (GPRS) load balancing, number of sessions associated with the real server. In per-packet server load balancing, number of request packets that have been load balanced to each real server, using the connection count.

The following is sample output from the **show ip slb reals detail** command for a dual-stack real server in a server farm:

```
Router# show ip slb reals detail

172.16.88.5, SF1, state = OPERATIONAL, type = server
  ipv6 = 2342:2342:2343:FF04:2388:BB03:3223:8912
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0
```

The following is sample output from the **show ip slb reals detail** command for a real server in a firewall farm:

```
Router# show ip slb reals detail

10.10.3.2, F, state = OPERATIONAL, type = firewall
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 8377, hash count = 0
  server failures = 0
  interface FastEthernet1/0, MAC 0000.0c41.1063
```

Table 33 describes the fields shown in the above detail displays.

Table 33 show ip slb reals detail Field Descriptions

Field	Description
IPv4 or IPv6 address	IPv4 or IPv6 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.
farm name	Name of the server farm or firewall farm with which the real server is associated.

Table 33 show ip slb reals detail Field Descriptions (continued)

state	Current state of the real server. • DFP_THROTTLED—The Dynamic Feedback Protocol (DFP) agent sent a weight of 0 for this real server (send no further connections to this real server). • FAILED—The real server has failed as a result of either no response or reset (RST) responses to client traffic. (See the **faildetect numconns (real server)** command for more information about controlling tolerance for no responses and RSTs.) The real server has been removed from use by the predictor algorithms. The retry timer has started. • MAXCONNS_THROTTLE—The number of connections on the real server exceeds the configured maximum number of simultaneous active connections (**maxconns**). • OPERATIONAL—The real server is functioning properly and is being used for load-balancing. • OPER_WAIT—The real server is waiting to become operational (waiting for a timeout or some other condition to be met). • OUTOFSERVICE—The real server was configured with **no inservice** and has been removed from the load-balancing predictor lists. • PROBE_FAILED—The probe has succeeded in the past but has currently failed. This failure might occur at the same time user connections fail, or it might not. • PROBE_TESTING—The probe has never succeeded, due to no response. The initial probe timed out waiting for a success. • READY_TO_TEST—The real server is queued for testing after being in FAILED state until the retry timer expired. • TESTING—The real server is queued for assignment. When a single user connection is assigned to a real server that is in READY_TO_TEST state, the real server is placed in TESTING state. If the test succeeds, the real server is placed back in OPERATIONAL state. • TEST_WAIT—The real server is waiting to begin testing (waiting for a timeout or some other condition to be met).
type	Indicates whether the real server is associated with a server farm (server) or firewall farm (firewall).
ipv6	IPv6 address of the real server about which information is being displayed, if dual-stack.
conns	Number of connections associated with the real server. In general packet radio service (GPRS) load balancing, number of sessions associated with the real server. In per-packet server load balancing, number of request packets that have been load balanced to each real server, using the connection count.
dummy_conns	Internal counter used in debugging.
maxconns	Maximum number of active connections allowed on the real server at one time.

Table 33 show ip slb reals detail Field Descriptions (continued)

weight	Weight assigned to the real server. The weight identifies the real server's capacity, relative to other real servers in the server farm. This value could be changed by DFP.
weight(admin)	Configured (or default) weight assigned to the real server.
metric	Internal counter used in debugging.
remainder	Internal counter used in debugging.
reassign	Total number of consecutive unacknowledged SYNchronize sequence numbers (SYNs) or Create Packet Data Protocol (PDP) requests since the last time the **clear ip slb counters** command was issued.
retry	Interval, in seconds, to wait between the detection of a failure on the real server and the next attempt to connect to the server.
rate	Maximum number of connections per second allowed on the real server.
failconn threshold	Maximum number of consecutive connection failures allowed before the real server is considered to have failed.
failconn count	Total number of consecutive connection failures since the last time the **clear ip slb counters** command was issued.
failclient threshold	Maximum number of unique client connection failures allowed before the real server is considered to have failed.
failclient count	Total number of unique client connection failures since the last time the **clear ip slb counters** command was issued.
total conns established	Total number of successful connection assignments since the last time the **clear ip slb counters** command was issued.
total conn failures	Total number of unsuccessful connection assignments since the last time the **clear ip slb counters** command was issued.
server failures	Total number of times this real server has been marked failed.
hash count	Total number of times the hash algorithm has been called.
interface	Type of interface.
MAC	MAC address of the firewall.

show ip slb replicate

To display the Cisco IOS Server Load Balancing (IOS SLB) replication configuration, use the **show ip slb replicate** command in privileged EXEC mode.

show ip slb replicate

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(2)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)ZA5	This command was modified to support slave replication.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip slb replicate** command:

```
Router# show ip slb replicate

VS1, state = NORMAL, interval = 10
 Slave Replication: Enabled
 Slave Replication statistics:
  unsent conn updates:         0
  conn updates received:       0
  conn updates transmitted:    0
  update messages received:    0
  update messages transmitted: 0
 Casa Replication:
  local = 10.1.1.1 remote = 10.2.2.2 port = 1024
  current password = <none> pending password = <none>
  password timeout = 180 sec (Default)
 Casa Replication statistics:
  unsent conn updates:        0
  conn updates received:      0
  conn updates transmitted:   0
  update packets received:    0
  update packets transmitted: 0
  failovers:                  0
```

Table 34 describes the fields shown in the display.

Table 34 show ip slb replicate Field Descriptions

Field	Description
state	Current replication state of the virtual server: • DUMPING—Dumping the connection table to the Hot Standby Router Protocol (HSRP) peer device. • NORMAL—Functioning properly. • PREEMPTING—Preparing to preempt the HSRP peer device and assume an active role.
interval	Replication buffering interval, in seconds.
Slave Replication	Indicates whether Slave Replication is enabled or disabled.
unsent conn updates	Number of Slave Replication or CASA Replication connection updates waiting to be sent.
conn updates received	Number of Slave Replication or CASA Replication connection updates received.
conn updates transmitted	Number of Slave Replication or CASA Replication connection updates sent.
update packets received	Number of Slave Replication or CASA Replication connection update packets received.
update packets transmitted	Number of Slave Replication or CASA Replication connection update packets sent.
local	Listening IP address for CASA Replication state exchange messages that are advertised.
remote	Destination IP address for all CASA Replication state exchange signals.
port	TCP or User Datagram Protocol (UDP) port number or port name for all CASA Replication state exchange signals.
current password	Current CASA Replication password for Message Digest Algorithm Version 5 (MD5) authentication, if any.
pending password	Pending CASA Replication password for MD5 authentication, if any.
failovers	Number of CASA Replication failovers detected.

Related Commands

Command	Description
request (HTTP probe)	Configures an HTTP probe to check the status of the real servers.

show ip slb serverfarms

To display information about the server farms, use the **show ip slb serverfarms** command in privileged EXEC mode.

show ip slb serverfarms [**name** *serverfarm-name*] [**detail**]

Syntax Description

name	(Optional) Displays information about only a particular server farm.
serverfarm-name	(Optional) Name of the server farm.
detail	(Optional) Displays detailed server farm 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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The output for the **detail** keyword was updated to display RADIUS load balancing enhancements and information about the IOS SLB KeepAlive Application Protocol (KAL-AP) agent.
15.0(1)S	The output for the **detail** keyword was updated to display the real server's IPv4, IPv6, or dual-stack address.

Examples

The following is sample output from the **show ip slb serverfarms** command:

```
Router# show ip slb serverfarms

server farm     predictor          nat   reals   bind id  interface(s)
GGSN            ROUNDROBIN         none  0       0        <any>
GGSN1           ROUNDROBIN         S     5       0        <any>
GGSN_IPV6       ROUNDROBIN         S     5       0        <any>
```

Table 35 describes the fields shown in the display.

Table 35 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, LEASTCONNS, or ROUTEMAP) used by the server farm
nat	NAT setting for the server farm: • **c**—Client NAT • **s**—Server NAT • **none**—NAT is not configured for the server farm
reals	Number of real servers configured in the server farm
bind id	Bind ID configured on the server farm.
interface(s)	Interface used by the server farm

The following is sample output from the **show ip slb serverfarms detail** command, if RADIUS load balancing is configured with the route map predictor:

```
Router# show ip slb serverfarms detail

SF1, predictor = ROUNDROBIN, nat =SERVER, interface(s) = Vl88
  virtuals inservice: 1, reals = 1, bind id = 0
  Real servers:
    172.16.88.5, weight = 8, OPERATIONAL, conns = 0
    ipv6 = 2342:2342:2343:FF04:2388:BB03:3223:8912
  Total connections = 0
```

For RADIUS load balancing with the route map predictor configured, specifying the **detail** keyword displays:

- **predictor = ROUTE-MAP**—Indicates that the **route-map** keyword is configured on the **predictor** command in SLB server farm configuration mode.
- **routemap name**—Name of the IOS policy-based routing (PBR) route map. If the route map is invalid or is not present, IOS SLB also displays **Not Configured/Valid**.

The following is sample output from the **show ip slb serverfarms detail** command, if a KAL-AP request was received for this server farm:

```
SF, predictor = ROUNDROBIN, nat = SERVER, interface(s) = <any>
  virtuals inservice: 1, reals = 2, bind id = 0
  KAL-AP tag: “chicago.com”, farm weight: 400
```

For the KAL-AP agent, specifying the **detail** keyword displays:

- **KAL-AP tag**—Domain tag to be used by the KAL-AP agent when searching for a server farm, if configured.
- **farm weight**—The weight to be used by the KAL-AP agent when calculating the load value for a server farm.

show ip slb sessions

To display information about sessions handled by Cisco IOS Server Load Balancing (IOS SLB), use the **show ip slb sessions** command in privileged EXEC mode.

show ip slb sessions [**asn** | **gtp** [**ipv6**] | **gtp-inspect** | **ipmobile** | **radius**] [**vserver** *virtual-server*] [**client** *ipv4-address ipv4-netmask*] [**detail**]

Syntax Description

asn	(Optional) Displays information about set of Access Service Network (ASN) gateways sessions being handled by IOS SLB.
gtp	(Optional) Displays IPv4 information about general packet radio service (GPRS) Tunneling Protocol (GTP) sessions being handled by IOS SLB.
ipv6	(Optional) Displays detailed information about the IPv6 sessions being handled by GTP load balancing.
gtp-inspect	(Optional) Displays information about GTP sessions being handled by IOS SLB that have GTP cause code inspection enabled.
ipmobile	(Optional) Displays information about Mobile IP sessions being handled by IOS SLB.
radius	(Optional) Displays information about RADIUS sessions being handled by IOS SLB.
vserver *virtual-server*	(Optional) Displays information about sessions being handled by the specified virtual server.
client *ipv4-address ipv4-netmask*	(Optional) Displays information about sessions associated with the specified client IPv4 address or subnet
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp** and **gtp-inspect** keywords were added.
12.2(14)ZA2	The **ipmobile** keyword was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC1	The **asn** keyword was added.
15.0(1)S	The **ipv6** keyword was added.

Examples

The following is sample output from the **show ip slb sessions** command for RADIUS sessions:

```
Router# show ip slb sessions radius

Source               Dest                   Retry
Addr/Port            Addr/Port           Id Count  Real            Vserver
-------------------------------------------------------------------------------
10.10.11.1/1645      10.10.11.2/1812     15     1  10.10.10.1  RADIUS_ACCT
```

Table 36 describes the fields shown in the display.

Table 36 show ip slb sessions radius Field Descriptions

Field	Description
Source Addr/Port	Source IPv4 address and port number for the session.
Dest Addr/Port	Destination IPv4 address and port number for the session.
Id	RADIUS identifier for the session.
Retry Count	Number of times a RADIUS request was sent by a RADIUS client without receiving a response from the RADIUS server (proxy or otherwise).
Real	IPv4 address of the SSG RADIUS server (proxy or otherwise).
Vserver	Name of the virtual server whose sessions are being monitored and displayed.

The following example shows GTP IPv4 session data:

```
Router# show ip slb sessions gtp

vserver         key              client          real                 state
-------------------------------------------------------------------------------
10.10.10.10     1234567890123456 10.5.5.5          10.10.1.1             GTP_ESTAB
```

Table 37 describes the fields shown in the display.

Table 37 show ip slb sessions gtp Field Descriptions

Field	Description
vserver	Name of the virtual server whose GTP sessions are being monitored and displayed. Information about each session is displayed on a separate line.
key	Network Service Access Point Identifier (NSAPI) key being used by the GTP session.
client	Client IPv4 address being used by the GTP session.
real	Real IPv4 address of the GTP session.
state	Current state of the GTP session: • **GTP_ESTAB**—The session has been established successfully. • **GTP_INIT**—The Packet Data Protocol (PDP) contexts have been deleted as a result of a delete request or a deletion in gateway GPRS support node (GGSN), and IOS SLB is waiting to destroy the session after the GTP_TIMEOUT. • **GTPIO_REQ_CLIENT**—Waiting for a response from the real server.

The following example shows GTP IPv6 session data:

```
Router# show ip slb sessions gtp ipv6

vserver = VS, key = 1112131415180030
  client = 3:3:3:3:3:3:3:9
  real = 4:4:4:4:4:4:4:4
  state = SLB_IPV6_GTP_ESTAB
```

The following example shows IOS SLB Mobile IP session data:

```
Router# show ip slb sessions ipmobile

vserver        NAI hash          client          real               retries
-------------------------------------------------------------------------------
VIRTUAL_HA     0xFFFF            10.1.1.1/434     10.10.1.1          1
```

Table 38 describes the fields shown in the display.

Table 38 show ip slb sessions ipmobile Field Descriptions

Field	Description
vserver	Name of the virtual server whose Mobile IP sessions are being monitored and displayed. Information about each session is displayed on a separate line.
NAI hash	Network access identifier (NAI) in the Registration Request (RRQ), used by Cisco IOS SLB as a unique identifier.
client	Client IPv4 address being used by the Mobile IP session.
real	Real IPv4 address of the Mobile IP session.
retries	Number of foreign agent retries for the Mobile IP session.

The following is sample output from the **show ip slb sessions asn** command for ASN sessions:

```
Router# show ip slb sessions asn

vserver         MSID              Base Station      real              state
-------------------------------------------------------------------------------
10.10.10.10     001646013fc0      5.5.5.5           10.10.1.1         ASN_REQ
```

Table 39 describes the fields shown in the display.

Table 39 show ip slb sessions asn Field Descriptions

Field	Description
vserver	Name of the virtual server whose ASN sessions are being monitored and displayed. Information about each session is displayed on a separate line.
MSID	Mobile Station Identifier (MSID), used by Cisco IOS SLB as a unique identifier.
Base Station	IPv4 address of the base station associated with the ASN session.

Table 39 show ip slb sessions asn Field Descriptions (continued)

real	Real IPv4 address of the ASN session.
state	Current state of the ASN session: • **ASN_ESTAB**—The session has been established successfully. • **ASN_INIT**—IOS SLB is waiting to destroy the session after timeouts in ASN_REQ or ASN_ESTAB state. If the base station is configured to send the ACK directly to the ASN gateway, and if **no faildetect inband** is configured, the session remains in ASN_REQ state until it is destroyed. • **ASN_REQ**—Waiting for a response from the real server.

show ip slb static

To display the Cisco IOS Server Load Balancing (IOS SLB) server Network Address Translation (NAT) configuration, use the **show ip slb static** command in privileged EXEC mode.

show ip slb static

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is to display the entire IOS SLB server NAT configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip slb static** command:

```
Router# show ip slb static

real                    action         address         counter
-----------------------------------------------------------------
10.11.3.4               drop           0.0.0.0         0
10.11.3.1               NAT            10.11.11.11     3
10.11.3.2               NAT sticky     10.11.11.12     0
10.11.3.3               NAT per-packet 10.11.11.13     0
```

Table 40 describes the fields shown in the display.

Table 40 show ip slb static Field Descriptions

Field	Description
real	IP address of the real server.

Table 40 show ip slb static Field Descriptions (continued)

action	Action to be taken by the real server: • drop—The real server is configured to have its packets dropped by IOS SLB, if the packets do not correspond to existing connections. • NAT—The real server is configured to use server NAT, and to use its own virtual IP address when translating addresses. • NAT per-packet—The real server is configured to use server NAT and per-packet server load balancing. • NAT sticky—The real server is configured to use server NAT for sticky connections. • pass-thru—The real server is not configured to use server NAT.
address	Virtual IP address used by the real server when translating addresses using server NAT. Address 0.0.0.0 means the real server is not configured for server NAT.
counter	For actions drop and NAT per-packet, indicates the number of packets processed by the real server. For actions NAT and NAT sticky, indicates the number of packets received by, but not necessarily processed by, the real server.

show ip slb stats

To display IOS Server Load Balancing (IOS SLB) statistics, use the **show ip slb stats** command in privileged EXEC mode.

show ip slb stats [kal-ap]

Syntax Description

kal-ap	(Optional) Displays information about the IOS SLB KeepAlive Application Protocol (KAL-AP) agent.

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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(9)E	This command was modified to support general packet radio service (GPRS) load balancing.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **kal-ap** keyword was added, and the output for the command was updated to display correlation inject failures for RADIUS load balancing accelerated data plane forwarding.
12.2(33)SRC1	The output for the command was updated to display packet fragment drops for Access Service Network (ASN) R6 load balancing.

Examples

The following is sample output from the **show ip slb stats** command:

```
Router# show ip slb stats
Pkts via normal switching:     108247
Pkts via special switching:    4307026
Pkts via slb routing:          1376241
Pkts Dropped:                  0
Connections Created:           933131
Connections Established:       350042
Connections Destroyed:         639323
Connections Reassigned:        0
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   2665
Failed Connection Allocs:      0
Failed Real Assignments:       0
```

```
RADIUS framed-ip Sticky Count: 524288
RADIUS username Sticky Count:  0
RADIUS cstn-id Sticky Count:   0
GTP imsi Sticky Count:         0
Route Flows Created:           1691177
Failed Route Flow Allocs:      0
Failed Correlation Injects:    0
Pkt fragments drops in ssv:    0
ASN MSID sticky count:         1
```

Table 41 describes the fields shown in the display.

Table 41 show ip slb stats Field Descriptions

Field	Description
Pkts via normal switching	Number of packets handled by IOS SLB via normal switching since the last time counters were cleared. Normal switching is when IOS SLB packets are handled on normal IOS switching paths (CEF, fast switching, and process level switching).
Pkts via special switching	Number of packets handled by IOS SLB via special switching since the last time counters were cleared. Special switching is when IOS SLB packets are handled on hardware-assisted switching paths.
Pkts via slb routing	Number of packets handled by IOS SLB via SLB routing since the last time counters were cleared.
Pkts dropped	Number of packets dropped or consumed by IOS SLB since the last time counters were cleared. The **Pkts dropped** field can increase for one or more of the following reasons: • Pings and other Internet Control Message Protocol (ICMP) packets addressed to a virtual IP address are dropped. • TCP data packets in which the **conn** entry is not available as a result of an idle timeout, failure of a probe, or failure of a real server, are dropped. • UDP traceroute packets addressed to a virtual IP address are dropped. • UDP packets addressed to a virtual IP address with a port number other than the one configured in the virtual server are dropped. If the virtual server uses the **any 0** port number, IOS SLB forwards the UDP packets to the real server. • Fragmented packets that cannot be reassembled are dropped.
Connections Created	Number of connections (or sessions, in general packet radio service [GPRS] load balancing and the Home Agent Director) created since the last time counters were cleared.
Connections Established	Number of connections (or sessions, in GPRS load balancing and the Home Agent Director) created and that have become established since the last time counters were cleared.

Table 41 show ip slb stats Field Descriptions (continued)

Connections Destroyed	Number of connections (or sessions, in GPRS load balancing and the Home Agent Director) destroyed since the last time counters were cleared.
Connections Reassigned	Number of connections (or sessions, in GPRS load balancing and the Home Agent Director) reassigned to a different real server since the last time counters were cleared.
Zombie Count	Number of connections (or sessions, in GPRS load balancing and the Home Agent Director) that are currently pending destruction (awaiting a timeout or some other condition to be met).
Connections Reused	Number of zombie connections (or sessions, in GPRS load balancing and the Home Agent Director) reused since the last time counters were cleared. A zombie connection is reused if it receives a TCP SYNchronize sequence number (SYN) or User Datagram Protocol (UDP) packet and succeeds in connecting to a real server. The zombie connection becomes a real connection and the zombie count is decremented.
Connection Flowcache Purges	Number of times the connection flow cache was purged since the last time counters were cleared.
Failed Connection Allocs	Number of times the allocation of a connection (or session, in GPRS load balancing) failed since the last time counters were cleared.
Failed Real Assignments	Number of times the assignment of a real server failed since the last time counters were cleared.
RADIUS framed-ip Sticky Count	Number of entries in the RADIUS framed-IP sticky database.
RADIUS username Sticky Count	Number of entries in the RADIUS username sticky database.
RADIUS cstn-id Sticky Count	Number of entries in the RADIUS calling-station-ID sticky database.
GTP imsi Sticky Count	Number of entries in the GTP IMSI sticky database.
Route Flows Created	Number of route flows created.
Failed Route Flows Allocs	Number of failed route flow allocations.
Failed Correlation Injects	Number of failed correlation injects.
Pkt fragments drops in ssv	Number of packet fragments drops in the SSV.
ASN MSID sticky count	Number of sticky objects in the ASN MSID sticky database.

The following is sample output from the **show ip slb kal-ap stats kal-ap** command:

```
Router# show ip slb kal-ap stats kal-ap

KAL-AP Mgr: (default), Socket state: OPEN, Socket retry: 0
KAL-AP Mgr: 2.2.2.2, Socket state: FAILED, Socket retry: 10
  UDP Port: 5002, vrf: vrf1
KAL-AP Mgr: 10.77.161.34, Socket state: FAILED, Socket retry: 10
  UDP Port: 5002, Secret: test
KAL-AP Packet Statistics:
Packet Received:     84
Bytes Received:      3966
```

```
Packet Sent:          30
Bytes Sent:           1080
Encrypt Errors:       0
Recv Failures:        0
Sent Failures:        0
KAL-AP Manager:       2.2.2.2     Secret:         Yes
KAL-AP Manager:       3.3.3.3     Secret:         Yes
CAPP UDP Port:        5001
Pkt Recd:             100         Bytes Recd:     12345
Pkt Sent:             100         Bytes Sent:     12121
MD5 checksum failed: 0            Error packets: 0
```

show ip slb sticky

To display the IOS Server Load Balancing (IOS SLB) sticky database, use the **show ip slb sticky** command in privileged EXEC mode.

show ip slb sticky [**asn** {**msid** *msid* | **nai** *nai*} | **client** *ipv4-address ipv4-netmask* | **gtp imsi** [**ipv6**] [**id** *imsi*] | **radius calling-station-id** [**id** *string*] | **radius framed-ip** [**client** *ipv4-address ipv4-netmask*] | **radius username** [**name** *string*]]

Syntax Description

asn msid *msid*	(Optional) Displays only those sticky database entries associated with the specified Access Service Network (ASN) Mobile Station ID (MSID).
asn nai *nai*	(Optional) Displays only those sticky database entries associated with the specified ASN network address identifier (NAI).
client *ipv4-address ipv4-netmask*	(Optional) Displays only those sticky database entries associated with the specified client IPv4 address or subnet.
gtp imsi	(Optional) Displays only entries associated with the IOS SLB general packet radio service (GPRS) Tunneling Protocol (GTP) International Mobile Subscriber ID (IMSI) sticky database, and shows all of the Network Service Access Point Identifiers (NSAPIs) that the user has used as primary Packet Data Protocols (PDPs).
ipv6	(Optional) Displays only IPv6 entries associated with the IOS SLB GTP IMSI sticky database, and shows all of the NSAPIs that the user has used as primary PDPs.
id *imsi*	(Optional) Displays only those sticky database entries associated with the specified IMSI.
radius calling-station-id	(Optional) Displays only entries associated with the IOS SLB RADIUS calling-station-ID sticky database.
id *string*	(Optional) Displays only those sticky database entries associated with the specified calling station ID.
radius framed-ip	(Optional) Displays only entries associated with the IOS SLB RADIUS framed-IP sticky database.
radius username	(Optional) Displays only entries associated with the IOS SLB RADIUS username sticky database.
name *string*	(Optional) Displays only those sticky database entries associated with the specified username.

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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(11b)E	The **radius** keyword was added.
12.1(12c)E	The **framed-ip**, **username**, **name**, *netmask*, and *string* keywords and arguments were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)ZA5	The **calling-station-id** and **id** keywords and the *string* argument were added.
12.2(18)SXE	The **gtp imsi** and **id** keywords and the *imsi* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	The **asn**, **msid**, and **nai** keywords and the *msid* and *nai* arguments were added.
15.0(1)S	The **ipv6** keyword was added. The output was updated to display the real server's GTP version and IPv4, IPv6, or dual-stack address.

Examples

The following is sample output from the **show ip slb sticky** command:

```
Router# show ip slb sticky

client           netmask          group  real                 conns
-------------------------------------------------------------------
10.10.2.12       255.255.0.0      4097   10.10.3.2            1
```

Table 42 describes the fields shown in the display.

Table 42 show ip slb sticky Field Descriptions

Field	Description
client	Client IPv4 address or subnet which is bound to this sticky assignment.
netmask	IPv4 subnet mask for this sticky assignment.
group	Group ID for this sticky assignment.
real	Real server used by all clients connecting with the client IPv4 address or subnet detailed on this line.
conns	Number of connections currently sharing this sticky assignment.

The following is sample output from the **show ip slb sticky gtp imsi** command:

```
Router# show ip slb sticky gtp imsi

IMSI                  Real         Ver  Group ID   vs_index  refcount  nsapi
-------------------------------------------------------------------------
11111111111111FF      10.10.10.1   1    5          10        1         6
11123411111111FF      10.10.10.2   1    5          10        1         9
```

Table 43 describes the fields shown in the display.

Table 43 show ip slb sticky gtp imsi Field Descriptions

Field	Description
IMSI	IMSI bound to this sticky assignment in the IOS SLB GTP IMSI sticky database.
Real	IPv4 address of the GTP IMSI real server.
Ver	GTP version: v0, v1, or v2
Group ID	Group ID for this sticky assignment.
vs_index	Virtual index, out of a maximum of 500.
refcount	Number of NSAPIs used as primary PDPs.
nsapi	NSAPI used as a primary PDP. **Note** IOS SLB does not display the **nsapi** column for GTP v2 sessions.

The following is sample output from the **show ip slb sticky gtp imsi ipv6** command:

```
Router# show ip slb sticky gtp imsi ipv6

IMSI             Real            Ver  Group Id  vs_index  refcount  NSAPIs
-------------------------------------------------------------------------
11121314151800F0 21.21.21.1      2    4099      7         1         3
                 2342:2342:2343:FF04:2342:AA03:2323:8912
```

The following is sample output from the **show ip slb sticky radius calling-station-id** command:

```
Router# show ip slb sticky radius calling-station-id

calling-station-id  group id     server real  framed-ips
-----------------------------------------------------
6228212             15           10.10.10.1   1
```

Table 44 describes the fields shown in the display.

Table 44 show ip slb sticky radius calling-station-id Field Descriptions

Field	Description
calling-station-id	Calling station ID bound to an SSG RADIUS proxy in the IOS SLB RADIUS calling-station-ID sticky database.
group id	Group ID for this sticky assignment.
server real	IPv4 address of the SSG RADIUS proxy server.
framed-ips	Number of IPv4 addresses bound to the SSG RADIUS proxy in the IOS SLB RADIUS framed-IP sticky database.

The following is sample output from the **show ip slb sticky radius framed-ip** command:

```
Router# show ip slb sticky radius framed-ip

framed-ip       group id     server real  route i/f
-----------------------------------------------------
1.1.1.1         15           10.10.10.1   <any>
```

Table 45 describes the fields shown in the display.

Table 45 show ip slb sticky radius framed-ip Field Descriptions

Field	Description
framed-ip	IPv4 address bound to a Cisco Service Selection Gateway (SSG) RADIUS proxy in the IOS SLB RADIUS framed-IP sticky database.
group id	Group ID for this sticky assignment.
server real	IPv4 address of the SSG RADIUS proxy server.
route i/f	Route interface.

The following is sample output from the **show ip slb sticky radius username** command:

```
Router# show ip slb sticky radius username

username        group id     server real  framed-ips
-----------------------------------------------------
9198783355      15           10.10.10.1   1
```

Table 46 describes the fields shown in the display.

Table 46 show ip slb sticky radius username Field Descriptions

Field	Description
username	Username bound to an SSG RADIUS proxy in the IOS SLB RADIUS username sticky database.
group id	Group ID for this sticky assignment.
server real	IPv4 address of the SSG RADIUS proxy server.
framed-ips	Number of IPv4 addresses bound to the SSG RADIUS proxy in the IOS SLB RADIUS framed-IP sticky database.

The following is sample output from the **show ip slb sticky asn** command:

```
Router# show ip slb sticky asn

MSID                Real      Group Id vs_index   NAI
-------------------------------------------------------
ABCD.12FE.3467   10.10.10.1   5         10        abc@cisco.com
2247.1130.8642   10.10.10.2   5         10        bcd@abc.com
```

Table 47 describes the fields shown in the display.

Table 47 show ip slb sticky asn Field Descriptions

Field	Description
MSID	MSID bound to this sticky assignment in the IOS SLB ASN sticky database.
Real	IPv4 address of the ASN real server.
Group ID	Group ID for this sticky assignment.
vs_index	Virtual index, out of a maximum of 500.
NAI	NAI bound to this sticky assignment in the IOS SLB ASN sticky database.

The following is sample output from the **show ip slb sticky asn nai abc@cisco.com** command:

```
Router# show ip slb sticky asn nai abc@cisco.com

MSID                Real      Group Id vs_index   NAI
-------------------------------------------------------
ABCD.12FE.3467   10.10.10.1   5         10        abc@cisco.com
```

Table 48 describes the fields shown in the display.

Table 48 show ip slb sticky asn nai abc@cisco.com Field Descriptions

Field	Description
MSID	MSID bound to this sticky assignment in the IOS SLB ASN sticky database.
Real	IPv4 address of the ASN real server.
Group ID	Group ID for this sticky assignment.
vs_index	Virtual index, out of a maximum of 500.
NAI	NAI bound to this sticky assignment in the IOS SLB ASN sticky database.

show ip slb vservers

To display information about the virtual servers, use the **show ip slb vservers** command in privileged EXEC mode.

show ip slb vservers [**name** *virtual-server*] [**redirect**] [**detail**]

Syntax Description

name *virtual-server*	(Optional) Displays information about the specified virtual server.
redirect	(Optional) Displays information about redirect virtual servers.
detail	(Optional) Displays detailed 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.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(18)SXF	The output for this command was modified to reflect the GTP sticky query option on the **idle (virtual server)** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The output for the **detail** keyword was updated to display information about the IOS SLB KeepAlive Application Protocol (KAL-AP) agent.
12.2(33)SRC1	The output for the **detail** keyword was updated to display information about Access Service Network (ASN) virtual servers.
15.0(1)S	The output was updated to display the virtual server's IPv4 or dual-stack address.

Usage Guidelines

If no options are specified, the command displays information about all virtual servers.

Examples

The following is sample output from the **show ip slb vservers** command:

```
Router# show ip slb vservers

slb vserver      prot  virtual              state         conns    interface(s)
-------------------------------------------------------------------------------
GGSN_SERVER1     UDP   4.3.2.1/32:0         OPERATIONAL   0        <any>
                       2342:2342:2343:FF04:2342:AA03:2323:8912/128
VS1              UDP   4.3.2.2/32:0         OPERATIONAL   0        <any>
                       2342:2342:2343:FF04:2343:AA03:2323:8912/128
VS2              UDP   4.3.2.3/32:0         OPERATIONAL   0        <any>
                       2342:2342:2343:FF04:2341:AA03:2323:8912/128
```

Table 49 describes the fields shown in the display.

Table 49 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.
virtual	Virtual IPv4 or dual-stack address of the virtual server, including the network mask, if configured.
state	Current state of the virtual server: • FAILED—Real server represented by this virtual server has been removed from use by the predictor algorithms; retry timer started. • OPERATIONAL—Functioning properly. • OUTOFSERVICE—Removed from the load-balancing predictor lists. • STANDBY—Backup virtual server, ready to become operational if active virtual server fails.
conns	Number of connections (or sessions, in general packet radio service [GPRS] load balancing and the Home Agent Director) associated with the virtual server.
interface	Type of interface.

The following sample output from the **show ip slb vservers detail** command shows detailed data for a virtual server with route health injection (advertise=TRUE):

```
Router# show ip slb vservers detail

VS, state = OPERATIONAL, v_index = 7, interface(s) = <any>
   virtual = 3.3.3.3/32:2123, UDP, service = GTP, advertise = TRUE
   ipv6 = 3:3:3:3:3:3:3:3/128
   serverfarm maps:
    map 1: priority = 1, serverfarm = SF, backup serverfarm= SF3
           ipv6 serverfarm = SF1 ipv6 backup serverfarm = SF2
    map 2: priority = 2, serverfarm = SF3, backup serverfarm= SF
          ipv6 serverfarm = SF2 ipv6 backup serverfarm = SF1
   serverfarm = <not assigned>, backup serverfarm = <not assigned>
   backup_serverfarm_hits = 0
   delay = 10, idle = 3600
   gtp: request idle = 30
        slb notification retry = 2
        gtp sticky query: <disabled>
        max retries: 0
   sticky: <none>
           group id = 0
   synguard counter = 0, synguard period = 0
   conns = 0, total conns = 0, syns = 0, syn drops = 0
   standby group = None
```

The following sample output from the **show ip slb vservers name detail** command shows detailed data for virtual server GGSN_SERVER with GTP sticky query enabled:

```
Router# show ip slb vservers name GGSN_SERVER detail

GGSN_SERVER, state = OPERATIONAL, v_index = 7, interface(s) = <any>
  virtual = 10.10.195.1/32:0, UDP, service = GTP, advertise = TRUE
```

```
server farm = GGSN, delay = 10, idle = 3600
gtp: request idle = 30, slb notification retry = 2
gtp sticky query: <enabled>, max retries: 3
sticky: <none>
sticky: group id = 4097 <assigned>
synguard counter = 0, synguard period = 0
conns = 0, total conns = 17192, syns = 0, syn drops = 0
standby group = None
```

Table 50 describes the fields shown in the display.

Table 50 show ip slb vservers name detail Field Descriptions

Field	Description
GGSN_SERVER	Name of the virtual server about which information is being displayed (in this case, GGSN_SERVER).
state	Current state of the virtual server: FAILED—Real server represented by this virtual server has been removed from use by the predictor algorithms; retry timer started. OPERATIONAL—Functioning properly. OUTOFSERVICE—Removed from the load-balancing predictor lists. STANDBY—Backup virtual server, ready to become operational if active virtual server fails.
v_index	Virtual index, out of a maximum of 500.
interface(s)	Type of interface.
virtual	Virtual IPv4 or dual-stack address of the virtual server, including the network mask, if configured.
UDP	Protocol being used by the virtual server (in this case, UDP).
service	Service, such as GTP, HTTP, or Telnet, associated with the virtual server (in this case, GTP).
advertise	Current state of host route advertisement for this virtual server: TRUE—Host route is being advertised. FALSE—Host route is not being advertised.
ipv6	For dual-stack, IPv6 address of the virtual server
server farm	Name of the server farm associated with the virtual server.
delay	Delay timer duration, in seconds, for this virtual server.
idle	Idle connection timer duration, in seconds, for this virtual server.
gtp request idle	GTP idle connection timer duration in seconds.
slb notification	Number of times IOS SLB can reassign a rejected Create PDP Context to a new real Cisco gateway GPRS support node (GGSN).
gtp sticky query	For GTP IMSI sticky, indicates whether IOS SLB is to query the GGSN before deleting any GTP IMSI sticky objects.
max retries	Maximum number of queries IOS SLB is to send to the GGSN when there is no response from the GGSN.
sticky	Indicates whether sticky connections are enabled for this virtual server.

Table 50 show ip slb vservers name detail Field Descriptions (continued)

sticky group id	Sticky group in which this virtual server is placed, for coupling of services.
synguard counter	Number of unacknowledged SYNchronize sequence numbers (SYNs) that are allowed to be outstanding to this virtual server.
synguard period	Interval, in milliseconds, for SYN threshold monitoring for this virtual server.
conns	Number of active connections currently associated with the virtual server.
total conns	Total number of connections that have been associated with the virtual server since coming INSERVICE.
syns	Number of SYNs handled by the virtual server in this period.
syn drops	Number of SYNs dropped by the virtual server in this period.
standby group	Hot Standby Router Protocol (HSRP) group name with which the virtual server is associated.

The following sample output from the **show ip slb vservers name detail** command shows detailed data for GTP virtual server GGSN_SERVER with maps enabled:

```
Router# show ip slb vservers name GGSN_SERVER detail
GGSN_SERVER, state = OPERATIONAL, v_index = 9, interface(s) = <any>
  virtual = 10.10.10.10/32:0, UDP, service = GTP, advertise = TRUE
  serverfarm maps:
  map 4: priority = 1, serverfarm = FARM4, backup = <none>
  map 1: priority = 3, serverfarm = FARM1, backup = FARM2
  map 5: priority = 4, serverfarm = FARM5, backup = <none>
  server farm = <not assigned>, delay = 10, idle = 3600
  gtp: request idle = 30, slb notification retry = 2
  gtp sticky query: <disabled>, max retries: 0
  sticky: <none>
  sticky: group id = 0
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 0, syns = 0, syn drops = 0
  standby group = None
```

Table 51 describes the fields shown in the display.

Table 51 show ip slb vservers name detail Field Descriptions

Field	Description
GGSN_SERVER	Name of the RADIUS virtual server about which information is being displayed (in this case, GGSN_SERVER).
state	Current state of the virtual server: FAILED—Real server represented by this virtual server has been removed from use by the predictor algorithms; retry timer started. OPERATIONAL—Functioning properly. OUTOFSERVICE—Removed from the load-balancing predictor lists. STANDBY—Backup virtual server, ready to become operational if active virtual server fails.
v_index	Virtual index, out of a maximum of 500.
interface(s)	Type of interface.

Table 51 show ip slb vservers name detail Field Descriptions (continued)

virtual	Virtual IPv4 or dual-stack address of the virtual server, including the network mask, if configured.
UDP	Protocol being used by the virtual server (in this case, UDP).
service	Service, such as GTP, HTTP, or Telnet, associated with the virtual server (in this case, GTP).
advertise	Current state of host route advertisement for this virtual server: TRUE—Host route is being advertised. FALSE—Host route is not being advertised.
serverfarm maps	List of IOS SLB server farm maps associated with this virtual server. Information about each map is displayed on a separate line.
priority	Priority of the map.
serverfarm	Server farm with which the map is associated.
backup	Backup server farm, if any.
server farm	Name of the server farm associated with the virtual server. Information about each server farm is displayed on a separate line.
map ID	Map associated with the server farm.
priority	Priority of the map.
delay	Delay timer duration, in seconds, for this virtual server.
idle	Idle connection timer duration, in seconds, for this virtual server.
gtp request idle	GTP idle connection timer duration in seconds.
slb notification	Number of times IOS SLB can reassign a rejected Create PDP Context to a new real Cisco gateway GPRS support node (GGSN).
gtp sticky query	For GTP IMSI sticky, indicates whether IOS SLB is to query the GGSN before deleting any GTP IMSI sticky objects.
max retries	Maximum number of queries IOS SLB is to send to the GGSN when there is no response from the GGSN.
sticky	Indicates whether sticky connections are enabled for this virtual server.
sticky group id	Sticky group in which this virtual server is placed, for coupling of services.
synguard counter	Number of unacknowledged SYNchronize sequence numbers (SYNs) that are allowed to be outstanding to this virtual server.
synguard period	Interval, in milliseconds, for SYN threshold monitoring for this virtual server.
conns	Number of active connections currently associated with the virtual server.
total conns	Total number of connections that have been associated with the virtual server since coming INSERVICE.
syns	Number of SYNs handled by the virtual server in this period.
syn drops	Number of SYNs dropped by the virtual server in this period.
standby group	Hot Standby Router Protocol (HSRP) group name with which the virtual server is associated.

The following sample output from the **show ip slb vservers name detail** command shows detailed data for an ASN virtual server:

```
Router# show ip slb vservers name ASN_VSERVER detail
ASN_VSERVER, state = OPERATIONAL, v_index = 10, interface(s) = <any>
  virtual = 2.2.2.2/32:0, UDP, service = ASNR6, advertise = TRUE
  server farm = SF, delay = 10, idle = 3600
  asn: request idle = 90
  asn: delete notif recvd = 2, nai-update notif recvd = 2
  asn: Notification Errors: Deletes = 1, nai-updates = 0
  sticky: <none>
  sticky: group id = 4097 <assigned>
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 156, syns = 0, syn drops = 0
  standby group = None
-------------------------------------------------------
                |      delete     |    nai-updates
   Real commn: |--------+--------+--------+-------------
  port = 63082 |  Recv  | Errors |  Recv  |  Errors
---------------+--------+--------+--------+-------------
    15.15.15.4       1         1        1         0
    15.15.15.5       1         0        1         0
```

Table 52 describes the fields shown in the display.

Table 52 show ip slb vservers name detail Field Descriptions

Field	Description
ASN_VSERVER	Name of the ASN virtual server about which information is being displayed (in this case, ASN_VSERVER).
state	Current state of the virtual server: FAILED—Real server represented by this virtual server has been removed from use by the predictor algorithms; retry timer started. OPERATIONAL—Functioning properly. OUTOFSERVICE—Removed from the load-balancing predictor lists. STANDBY—Backup virtual server, ready to become operational if active virtual server fails.
v_index	Virtual index, out of a maximum of 500.
interface(s)	Type of interface.
virtual	Virtual IPv4 or dual-stack address of the virtual server, including the network mask, if configured.
UDP	Protocol being used by the virtual server (in this case, UDP).
service	Service, such as GTP, HTTP, or Telnet, associated with the virtual server (in this case, ASNR6).
advertise	Current state of host route advertisement for this virtual server: TRUE—Host route is being advertised. FALSE—Host route is not being advertised.

Table 52 show ip slb vservers name detail Field Descriptions (continued)

server farm	Name of the server farm associated with the virtual server. Information about each server farm is displayed on a separate line.
delay	Delay timer duration, in seconds, for this virtual server.
idle	Idle connection timer duration, in seconds, for this virtual server.
asn: request idle	ASN idle connection timer duration in seconds.
asn: delete notif recvd	Number of delete notifications received.
asn: nai-update notif recvd	Number of NAI-update notifications received.
asn: Notification Errors: Deletes	Number of delete notification errors.
asn: Notification Errors: nai-updates	Number of NAI-update notification errors.
sticky	Indicates whether sticky connections are enabled for this virtual server.
sticky group id	Sticky group in which this virtual server is placed, for coupling of services.
synguard counter	Number of unacknowledged SYNchronize sequence numbers (SYNs) that are allowed to be outstanding to this virtual server.
synguard period	Interval, in milliseconds, for SYN threshold monitoring for this virtual server.
conns	Number of active connections currently associated with the virtual server.
total conns	Total number of connections that have been associated with the virtual server since coming INSERVICE.
syns	Number of SYNs handled by the virtual server in this period.
syn drops	Number of SYNs dropped by the virtual server in this period.
standby group	Hot Standby Router Protocol (HSRP) group name with which the virtual server is associated.
Real commn: port	Port used by the real server.

show ip slb wildcard

To display information about the wildcard representation for irtual servers, use the **show ip slb wildcard** command in privileged EXEC mode.

show ip slb wildcard

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.0(1)S	The output was updated to display the virtual server's IPv4, IPv6, or dual-stack address.

Examples

The following is sample output from the **show ip slb wildcard** command:

```
Router# show ip slb wildcard

Interface Source Address         Port  Destination Address    Port  Prot
ANY       0.0.0.0/0              0     3.3.3.3/32             2123  UDP
ANY       0.0.0.0/0              0     3.3.3.3/32             0     UDP
ANY       0.0.0.0/0              0     0.0.0.0/0              0     ICMP

Interface: ANY
Source Address [Port]: ::/0[0]
Destination Address [Port]: 2342:2342:2343:FF04:2341:AA03:2323:8912/128[0]
Protocol: ICMPV6

Interface: ANY
Source Address [Port]: ::/0[0]
Destination Address [Port]: 2342:2342:2343:FF04:2341:AA03:2323:8912/128[2123]
Protocol: UDP
```

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 arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0 T	This command was introduced.
12.2(2)T	Support for IPv6 socket information in the display output of the command was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was replaced by the **show udp**, **show sockets** and **show ip sctp** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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      10.0.0.0          0       172.16.186.193  67    0   0    1   0
 17      172.16.191.135    514     172.16.191.129  1811  0   0    0   0
 17      172.16.135.20     514     172.16.191.1    4125  0   0    0   0
 17      172.16.207.163    49      172.16.186.193  49    0   0    9   0
 17      10.0.0.0          123     172.16.186.193  123   0   0    1   0
 88      10.0.0.0          0       172.16.186.193  202   0   0    0   0
 17      172.16.96.59      32856   172.16.191.1    161   0   0    1   0
 17     --listen--              --any--        496  0    0   1    0
```

The following sample output from the **show ip sockets** command shows IPv6 socket information:

```
Router# show ip sockets

Proto      Remote     Port     Local      Port      In      Out      Stat      TTY OutputIF
17(v6)   --listen--           --any--    1024       0       0         0        0
17(v6)   --listen--           --any--       7       0       0         0        0
17(v6)   --listen--           --any--     161       0       0         0        0
17(v6)   --listen--           --any--     162       0       0         0        0
17       --listen--           --any--    1024       0       0         0        0
17       --listen--           --any--       7       0       0         0        0
17       --listen--           --any--       9       0       0         0        0
17       --listen--           --any--      19       0       0         0        0
17       --listen--           --any--    1645       0       0         0        0
17       --listen--           --any--    1646       0       0         0        0
17       --listen--           --any--     161       0       0         0        0
17       --listen--           --any--     162       0       0         0        0
```

Table 53 describes the significant fields shown in the display.

Table 53 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.
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.
v6	IPv6 sockets.

Related Commands

Command	Description
show ip sctp	Displays information about SCTP.
show processes	Displays information about the active processes.
show sockets	Displays IP socket information.
show udp	Displays IP socket information about UDP processes.

show ip tcp header-compression

To display TCP/IP header compression statistics, use the **show ip tcp header-compression** command in user EXEC or privileged EXEC mode.

show ip tcp header-compression [*interface-type interface-number*] [**detail**]

Syntax Description

interface-type interface-number	(Optional) The interface type and number.
detail	(Optional) Displays details of each connection. This keyword is available only in privileged EXEC mode.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.4	This command was integrated into Cisco Release 12.4 and its command output was modified to include additional compression statistics.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(15)T12	This command was modifed. Support was added for the special Van Jacobson (VJ) format of TCP header compression.

Examples

The following is sample output from the **show ip tcp header-compression** command:

```
Router# show ip tcp header-compression

TCP/IP header compression statistics:
  Interface Serial2/0 (compression on, IETF)
    Rcvd:    53797 total, 53796 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    53797 total, 53796 compressed, 0 status msgs, 0 not predicted
             1721848 bytes saved, 430032 bytes sent
             5.00 efficiency improvement factor
    Connect: 16 rx slots, 16 tx slots,
             1 misses, 0 collisions, 0 negative cache hits, 15 free contexts
             99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

Table 54 describes the significant fields shown in the display.

Table 54 show ip tcp header-compression Field Descriptions

Field	Description
Interface Serial2/0 (compression on, IETF)	Interface type and number on which compression is enabled.
Rcvd:	Received statistics described in subsequent fields.
total	Total number of TCP packets received on the interface.
compressed	Total number of TCP packets compressed.
errors	Number of packets received with errors.
status msgs	Number of resynchronization messages received from the peer.
dropped	Number of packets dropped due to invalid compression.
buffer copies	Number of packets that needed to be copied into bigger buffers for decompression.
buffer failures	Number of packets dropped due to a lack of buffers.
Sent:	Sent statistics described in subsequent fields.
total	Total number of TCP packets sent on the interface.
compressed	Total number of TCP packets compressed.
status msgs	Number of resynchronization messages sent from the peer.
not predicted	Number of packets taking a nonoptimal path through the compressor.
bytes saved	Total savings in bytes due to compression.
bytes sent	Total bytes sent after compression.
efficiency improvement factor	Improvement in line efficiency because of TCP header compression, expressed as the ratio of total packet bytes to compressed packet bytes. The ratio should be greater than 1.00.
Connect:	Connection statistics described in subsequent fields.
rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
misses	Indicates the number of times a match could not be made. If your output shows a large miss rate, then the number of allowable simultaneous compression connections may be too low.
collisions	Total number of collisions.
negative cache hits	Total number of negative cache hits. **Note** This field is not relevant for TCP header compression; it is used for Real-Time Transport Protocol (RTP) header compression.
free contexts	Total number of free contexts. **Note** Free contexts (also known as connections) are an indication of the number of resources that are available, but not currently in use, for TCP header compression.
hit ratio	Percentage of times the software found a match and was able to compress the header.

Table 54 show ip tcp header-compression Field Descriptions (continued)

Field	Description
Five minute miss rate 0 misses/sec	Calculates the miss rate over the previous five minutes for a longer-term (and more accurate) look at miss rate trends.
max	Maximum value of the previous field.

The following example for Cisco IOS Release 12.4(15)T12 shows that the TCP special VJ format is enabled:

```
Router# show ip tcp header-compression serial 5/0 detail

TCP/IP header compression statistics:
 DLCI 100        Link/Destination info: ip 10.72.72.2
Configured:
 Max Header 60 Bytes, Max Time 50 Secs, Max Period 32786 Packets, Feedback On, Spl-VJ On
Negotiated:
 Max Header 60 Bytes, Max Time 50 Secs, Max Period 32786 Packets, Feedback On, Spl-VJ On
TX contexts:
```

Related Commands

Command	Description
ip header-compression special-vj	Enables the special VJ format of TCP header compression.
ip tcp compression-connections	Specifies the total number of TCP header compression connections that can exist on an interface
special-vj	Enables the special VJ format of TCP header compression so that context IDs are included in compressed packets.

show ip traffic

To display the global or system-wide IP traffic statistics for one or more interfaces, use the **show ip traffic** command in user EXEC or privileged EXEC mode.

show ip traffic [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays the global or system-wide IP traffic statistics for a specific interface. If the **interface** keyword is used, the *type* and *number* arguments are required.

Command Default

Using the **show ip traffic** command with no keywords or arguments displays the global or system-wide IP traffic statistics for all interfaces.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2	The output was enhanced to display the number of keepalive, open, update, route-refresh request, and notification messages received and sent by a Border Gateway Protocol (BGP) routing process.
12.2(25)S	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXH5	This command was modified. The output was changed to display the ARP (proxy) reply counter as the number of ARP replies for real proxies only.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S. This command was modified to include the optional **interface** keyword and associated *type* and *number* arguments. These modifications were made to provide support for the IPv4 MIBs as described in RFC 4293: *Management Information Base for the Internet Protocol (IP)*.

Usage Guidelines

Using the **show ip traffic** command with the optional **interface** keyword displays the ipIfStatsTable counters for the specified interface if IPv4 addressing is enabled.

Examples

The following is sample output from the **show ip traffic** command:

```
Router# show ip traffic

IP statistics:
  Rcvd:  27 total, 27 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, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 27 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  0 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
  Drop:  0 packets with source IP address zero

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
        0 irdp solicitations, 0 irdp advertisements
        0 time exceeded, 0 timestamp replies, 0 info replies
  Sent: 0 redirects, 0 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
        0 irdp solicitations, 0 irdp advertisements

BGP statistics:
  Rcvd: 0 total, 0 opens, 0 notifications, 0 updates
        0 keepalives, 0 route-refresh, 0 unrecognized
  Sent: 0 total, 0 opens, 0 notifications, 0 updates
        0 keepalives, 0 route-refresh

EIGRP-IPv4 statistics:
  Rcvd: 0 total
  Sent: 0 total

TCP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total

PIMv2 statistics: Sent/Received
  Total: 0/0, 0 checksum errors, 0 format errors
  Registers: 0/0 (0 non-rp, 0 non-sm-group), Register Stops: 0/0,  Hellos: 0/0
  Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
  Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0
  State-Refresh: 0/0

IGMP statistics: Sent/Received
  Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
  Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
  DVMRP: 0/0, PIM: 0/0

UDP statistics:
  Rcvd: 185515 total, 0 checksum errors, 185515 no port
  Sent: 0 total, 0 forwarded broadcasts
```

```
OSPF statistics:
  Rcvd: 0 total, 0 checksum errors
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks

  Sent: 0 total
        0 hello, 0 database desc, 0 link state req
        0 link state updates, 0 link state acks

Probe statistics:
  Rcvd: 0 address requests, 0 address replies
        0 proxy name requests, 0 where-is requests, 0 other
  Sent: 0 address requests, 0 address replies (0 proxy)
        0 proxy name replies, 0 where-is replies

ARP statistics:
  Rcvd: 1477 requests, 8841 replies, 396 reverse, 0 other
  Sent: 1 requests, 20 replies (0 proxy), 0 reverse
  Drop due to input queue full: 0
```

Cisco 10000 Series Routers Example

The following is sample output from the **show ip traffic** command when used on a Cisco 10000 series router:

```
Router# show ip traffic

IP statistics:
  Rcvd:  27 total, 27 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, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 couldn't fragment
  Bcast: 27 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  0 generated, 0 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop
         0 options denied, 0 source IP address zero
```

Table 55 describes the significant fields shown in the display.

Table 55 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 Address Resolution Protocol (ARP) request entry and therefore did not send a datagram.
no route	Counted when the Cisco IOS software discards a datagram that it did not know how to route.

Related Commands

Command	Description
clear ip traffic	Clears the global or system-wide IP traffic statistics for one or more interfaces.

show ip wccp

To display the Web Cache Communication Protocol (WCCP) global configuration and statistics, use the **show ip wccp** command in user EXEC or privileged EXEC mode.

show ip wccp [**summary**] [**capabilities**] [**vrf** *vrf-name*] [*service-number* | **interfaces** [**cef** | **counts** | **detail**] | **web-cache** | **all** [**view** | {**assignment** | **service** | **clients** [**id** *ip-address*] | **full** | **detail** [**counters**] [**internal**]}]

Syntax Description

summary	(Optional) Displays a summary of WCCP services.
capabilities	(Optional) Displays WCCP platform capabilities information.
vrf *vrf-name*	(Optional) Specifies a VRF associated with a service group to display.
service-number	(Optional) Identification number of the web cache service group being controlled by the cache. The number can be from 0 to 254. For web caches using Cisco cache engines, the reverse proxy service is indicated by a value of 99.
interfaces	(Optional) WCCP redirect interfaces.
cef	(Optional) CEF interface statistics, including the number of input, output, dynamic, static, and multicast services.
counts	(Optional) WCCP interface count statistics, including the number of CEF and process-switched output and input packets redirected.
detail	(Optional) WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
web-cache	(Optional) Statistics for the web cache service.
all	(Optional) Statistics for all known services.
view	(Optional) Other members of a particular service group, or all service groups, have or have not been detected.
assignment	(Optional) Service group assignment information.
service	(Optional) Detailed information about a service, including the service definition and all other per-service information.
clients	(Optional) Detailed information about the clients of a service, displaying all per-client information. No per-service information or traffic counters are displayed.
id *ip-address*	(Optional) Restricts the output to display per-client information relating only to the specified client, instead of all clients of the service. If the specified client does not exist, no output is displayed.
full	(Optional) Detailed information about a service and all the clients of the service. Displays the per-service information and all of the per-client information.
detail	(Optional) Information about the router and all web caches.
counters	(Optional) Displays traffic counters.
internal	(Optional) Displays internal information. This output is considered useful only to Cisco IOS developers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.1CA	This command was introduced for Cisco 7200 and 7500 platforms.
11.2P	Support for this command was added to a variety of Cisco platforms.
12.0(3)T	The **detail** and **view** 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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	The output was enhanced to display the maximum number of service groups.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was enhanced to display information about the WCCP service mode.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.
15.0(1)M	This command was modified. The **summary** keyword and the **vrf** *vrf-name* keyword and argument pair were added.
12.2(33)SRE	This command was modified. The **summary** keyword and the **vrf** *vrf-name* keyword and argument pair were added.
Cisco IOS XE Release 3.1S	This command was modified. The following keywords and arguments were added: **all**, **assignment**, **summary**, **service**, **clients**, **full**, **capabilities**, **counters**, **id** *ip-address*, **vrf** *vrf-name*.

Usage Guidelines

Use the **clear ip wccp** command to reset the counter for the “Packets Redirected” information.

Use the **show ip wccp** *service-number* command to provide the “Total Packets Redirected” count. The “Total Packets Redirected” count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp** *service-number* **detail** command to provide the “Packets Redirected” count. The “Packets Redirected” count is the number of flows, or sessions, that are redirected.

Use the **show ip wccp web-cache detail** command to provide an indication of how many flows, rather than packets, are using Layer 2 redirection.

Use the **show ip wccp summary** command to show the configured WCCP services and a summary of their current state.

For cache-engine clusters using Cisco cache engines, the reverse proxy *service-number* is indicated by a value of 99.

On Cisco ASR 1000 Series Routers, nonzero values can only be seen for platform-specific counters because Cisco ASR 1000 Series Routers implement all redirection in hardware. Configuring the **counters** keyword also displays counters received in hardware.

Examples

This section contains examples and field descriptions for the following forms of this command:

- **show ip wccp** *service-number* (service mode displayed)
- **show ip wccp** *service-number* **view**
- **show ip wccp** *service-number* **detail**
- **show ip wccp interfaces**
- **show ip wccp web-cache**
- **show ip wccp web-cache counters**
- **show ip wccp web-cache detail**
- **show ip wccp web-cache detail** (bypass counters displayed)
- **show ip wccp web-cache service**
- **show ip wccp summary**

show ip wccp *service-number* (Service Mode Displayed)

The following is sample output from the **show ip wccp** *service-number* command:

```
Router# show ip wccp 90

Global WCCP information:
    Router information:
        Router Identifier:                  100.1.1.16
        Protocol Version:                   2.0

    Service Identifier: 90
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       0
          Process:                          0
          CEF:                              0
        Service mode:                       Closed
        Service Access-list:                tcp91
        Total Packets Dropped Closed:       0
        Redirect Access-list:               -none-
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group Access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
```

Table 56 describes the significant fields shown in the display.

*Table 56 **show ip wccp** service-number **Field Descriptions***

Field	Description
Router information	A list of routers detected by the current router.
Protocol Version	The version of WCCP being used by the router in the service group.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients:	The number of clients that are visible to the router and other clients in the service group.
Number of Service Group Routers	The number of routers in the service group.

*Table 56 **show ip wccp** service-number **Field Descriptions (continued)***

Field	Description
Total Packets s/w Redirected	Total number of packets redirected by the router.
Service mode: Closed	Identifies the WCCP service mode. Options are open or closed.
Service Access-list	A named extended IP access list that defines the packets that will match the service.
Total Packets Dropped Closed	Total number of packets that were dropped when WCCP is configured for closed services and an intermediary device is not available to process the service.
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 packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.
Total Bypassed Packets Received	The number of packets that have been bypassed. Process, fast, and Cisco Express Forwarding (CEF) are switching paths within Cisco IOS software.

show ip wccp *service-number* **view**

The following is sample output from the **show ip wccp** *service-number* **view** command for service group 1:

```
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-
```

Note The number of maximum service groups that can be configured is 256.

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 57 describes the significant fields shown in the display.

Table 57 show ip wccp** service-number **view Field Descriptions

Field	Description
WCCP Router Informed of	A list of routers detected by the current router.
WCCP Clients Visible	A list of clients that are visible to the router and other clients in the service group.
WCCP Clients Not Visible	A list of clients in the service group that are not visible to the router and other clients in the service group.

show ip wccp *service-number* detail

The following example displays WCCP client information and WCCP router statistics that include the type of services:

```
Router# show ip wccp 91 detail

WCCP Client information:
 WCCP Client ID: 10.1.1.14
 Protocol Version: 2.0
 State: Usable
 Redirection: GRE
 Packet Return: GRE
 Assignment: HASH
 Initial Hash Info: 00000000000000000000000000000000000000000000000000000000000000000000
 Assigned Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
 Hash Allotment: 256 (100.00%)
 Packets Redirected: 0
 Connect Time: 00:01:56
 Bypassed Packets
 Process: 0
 CEF: 0
```

show ip wccp interfaces

The following is sample output from the **show ip wccp interfaces** command:

```
Router# show ip wccp interfaces

WCCP interface configuration:
    FastEthernet0/1/0
        Output services: 2
        Input services: 3
        Mcast services: 1
        Exclude In:      FALSE
```

Table 58 describes the significant fields shown in the display.

Table 58 show ip wccp interfaces Field Descriptions

Field	Description
Output services	Indicates the number of output services configured on the interface.
Input services	Indicates the number of input services configured on the interface.

Table 58 show ip wccp interfaces Field Descriptions (continued)

Field	Description
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

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:
    Router information:
        Router Identifier:                   R1
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Service Group Clients:     0
        Number of Service Group Routers:     0
        Total Packets Redirected:            213
          Process:                           0
          CEF:                               0
          Platform:                          0
        Service mode:                        Open
        Service Access-list:                 -none-
        Total Packets Dropped Closed:        0
        Redirect access-list:                no_linux
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
          Platform:                          0
```

Table 59 describes the significant fields shown in the display.

Table 59 show ip wccp web-cache Field Descriptions

Field	Description
Protocol Version	Indicates whether WCCPv1 or WCCPv2 is enabled.
Service Identifier	Indicates which service is detailed.
Number of Service Group Clients	Number of clients using the router as their home router.
Number of Service Group Routers	The number of routers in the service group.
Total Packets Redirected	Total number of packets redirected by the router.
Service mode	Indicates whether WCCP open or closed mode is configured.
Service Access-list	The name or number of the service access list that determines which packets will be redirected.
Redirect access-list	The name or number of the access list that determines which packets will be redirected.

Table 59 show ip wccp web-cache Field Descriptions (continued)

Field	Description
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 packets denied by the *group-list* access list.
Total Authentication failures	The number of instances where a password did not match.

show ip wccp web-cache counters

The following example displays web cache engine information and WCCP traffic counters:

```
Router# show ip wccp web-cache counters

WCCP Service Group Counters:
   Redirected Packets:
     Process:                     4
     CEF:                         5
   Non-Redirected Packets:
     Action - Forward:
       Reason - no assignment:
         Process:                 2
         CEF:                     1
     Action - Ignore (forward):
       Reason - redir ACL check:
         Process:                 2
         CEF:                     3
Action - Discard:
Reason - closed services:
Process:                          0
CEF:                              0
GRE Bypassed Packets:
  Process:                        4
  CEF:                            5
GRE Bypassed Packet Errors:
  Total Errors:
    Process:                      0
    CEF:                          0

WCCP Client Counters:
  WCCP Client ID: 10.1.1.82
    Redirect Assignments:
      Received:                   1
      Invalid:                    0
      Duplicate:                  0
Redirected Packets:
  Process:                        4
  CEF:                            5
GRE Bypassed Packets:
  Process:                        4
  CEF:                            5
```

Table 60 describes the significant fields shown in the display.

Table 60 show ip wccp web-cache counters Field Descriptions

Field	Description
Redirected Packets	Total number of packets redirected by the router.
Non-Redirected Packets	Total number of packets not redirected by the router.
Platform	Total number of packets redirected or not redirected in hardware.

show ip wccp web-cache detail

The following example displays web cache engine information and WCCP router statistics for the web cache service:

```
Router# show ip wccp web-cache detail

WCCP Client information:
        WCCP Client ID:          10.20.1.10 (IP address: 10.20.1.2)
        Protocol Version:        2.0
        State:                   Usable
        Redirection:             L2
        Packet Return:           GRE
        Assignment:              MASK
        Connect Time:            00:18:22
        Redirected Packets:
          Process:               0
          CEF:                   0
          Platform:              39
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          64 of 64 (100.00%)

        Mask  SrcAddr    DstAddr    SrcPort DstPort
        ----  -------    -------    ------- -------
        0000: 0x00001741 0x00000000 0x0000  0x0000

        Value SrcAddr    DstAddr    SrcPort DstPort
        ----- -------    -------    ------- -------
        0000: 0x00000000 0x00000000 0x0000  0x0000
        0001: 0x00000001 0x00000000 0x0000  0x0000
        0002: 0x00000040 0x00000000 0x0000  0x0000
        0003: 0x00000041 0x00000000 0x0000  0x0000
.
.
.
```

Table 61 describes the significant fields shown in the display.

Table 61 show ip wccp web-cache detail Field Descriptions

Field	Description
WCCP Client Information	The header for the area that contains fields for information on clients.
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.

Table 61 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.
Packets Redirected	The number of packets that have been redirected to the cache engine.
Connect Time	The amount of time the cache engine has been connected 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 Client Information
 IP Address:10.168.88.11
 Protocol Version:2.0
 State:Usable
 Initial Hash Info:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 Assigned Hash Info:FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
 Hash Allotment:256 (100.00%)
 Packets Redirected:21345
 Connect Time:00:13:46
Bypassed Packets
 Process:             0
 Fast:                0
 CEF:                 250
```

Table 62 describes the significant fields shown in the display.

Table 62 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 Client Information	The header for the area that contains fields for information on clients.
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 62 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 the cache engine has been connected 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.

show ip wccp web-cache service

The following example displays information about a service, including the service definition and all other per-service information:

```
Router# show ip wccp web-cache service

WCCP service information definition:
        Type:          Standard
        Id:            0
        Priority:      240
        Protocol:      6
        Options:       0x00000512
        --------
            Mask/Value sets: 1
            Value elements: 4
            Dst Ports: 80 0 0 0 0 0 0 0
```

show ip wccp summary

The following example displays information on the configured WCCP services and a summary of their current state:

```
Router# show ip wccp summary

WCCP version 2 enabled, 2 services

Service     Clients   Routers   Assign      Redirect   Bypass
-------     -------   -------   ------      --------   ------
Default routing table (Router Id: TBD):
90          0         0         HASH/MASK   GRE/L2     GRE/L2
VRF red (Router Id: 10.1.1.1):
90          1         1         HASH        L2         GRE
```

Table 63 describes the significant fields shown in the display.

Table 63 show ip wccp summary detail Field Descriptions

Field	Description
Service	Indicates which service is detailed.
Clients	Indicates the number of cache engines participating in the WCCP service.
Routers	Indicates the number of routers participating in the WCCP service.
Assign	Indicates the load-balancing method used. WCCP uses Hash or Mask assignment.
Redirect	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Bypass	Indicates the bypass method used. WCCP uses GRE or L2 to return packets to the router.

Related Commands

Command	Description
clear ip wccp	Clears the counter for packets redirected using WCCP.
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
ip wccp web-cache accelerated	Enables the hardware acceleration for WCCP version 1.
show ip interface	Lists a summary of the IP information and status of an interface.
show ip wccp global counters	Displays global WCCP information for packets that are processed in software.
show platform software wccp	Displays global statistics related to WCCP on Cisco ASR 1000 Series Routers.

show ip wccp global counters

To display global Web Cache Communication Protocol (WCCP) information for packets that are processed in software, use the **show ip wccp global counters** command in user EXEC or privileged EXEC mode.

show ip wccp global counters

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ip wccp global** command displays counters for packets that are processed in software. These counters are always zero on the Cisco ASR 1000 Series Routers.

Examples

The following example displays global WCCP information for packets that are processed in the software:

```
Router# show ip wccp global counters

WCCP Global Counters:

Packets Seen by WCCP
Process:   8
CEF (In):  14
CEF (Out): 0
```

Related Commands

Command	Description
clear ip wccp	Clears the counters for packets redirected using WCCP.
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
ip wccp web-cache accelerated	Enables the hardware acceleration for WCCP version 1.
show ip interface	Lists a summary of the IP information and the status of an interface.
show ip wccp	Displays the WCCP global configuration and statistics.

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.

show platform hardware qfp active feature wccp

To display the Web Cache Communication Protocol (WCCP) service group information in the active Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active feature wccp** command in privileged EXEC mode.

show platform hardware qfp active feature wccp [**vrf** *vrf-id*] **service id** *service-id*

Syntax Description

vrf *vrf-id*	(Optional) Specifies a VRF associated with a service group to display.
service id *service-id*	Specifies the WCCP service group ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Examples

The following is a sample output from the **show platform hardware qfp active feature wccp** command:

```
Router# show platform hardware qfp active feature wccp service id 1

Service ID: 0
Service Priority: 240
CG ID: 0
Mode: Open
Num bind objs: 64
Number of Caches in this service: 1
  ce index: 0
  cache_id : 15
  Cache ip addr : 0x5a140102
  Cache cfg ppe addr : 0x8b480000
  Cache oce ppe addr : 0x89b01480
  Cache state ppe addr : 0x8b4d0400
Number of interfaces using this service: 1
  Interface: GigabitEthernet0/3/1
  cpp-if-h: 18
  Dir: 0
  pal-if-h: 20
```

Table 64 describes the significant fields shown in the display.

Table 64 show platform hardware qfp active feature wccp Field Descriptions

Field	Description
Service ID	Service group number (0 for webcache and 1 to 254 for dynamic services).
Service Priority	Priority of the service group.
CG ID	Class Group ID, which is the same value as the Service ID.
Mode	Specifies whether the service group has been defined as an open service group (default value) or closed service group.
Num bind objs	Number of access control entries (ACEs) in the merged access control list (ACL) for this service group. On the Quantum Flow Processor (QFP), each ACE is programmed as a bind object under a class group specified by the CG ID.
Number of Caches in this service	The number of cache engines available for this service group.
Number of interfaces using this service	The number of interfaces on which this service group has been configured (both inbound as well as outbound redirection).

show platform software wccp

To display platform specific configuration and statistics related WCCP information on Cisco ASR 1000 Series Routers, use the **show platform software wccp** command in privileged EXEC mode.

show platform software wccp [*service-number* **counters** | [*slot* [*service-number* [**access-list**] | **cache-info** | **interface** | **statistics** | **web-cache** [**access-list**]] | [**vrf** *vrf-identifier* {*service-number* [**access-list**] | **web-cache** [**access-list**]}]] | **interface counters** | **statistics** | [**vrf** *vrf-identifier* {*service-number* **counters** | **web-cache counters**}] | **web-cache counters**]

Syntax Description

service-number	(Optional) Displays information for a dynamically defined service. The service number can be from 0 to 254.
counters	(Optional) Displays counter information.
slot	(Optional) Embedded Service Processor or Route Processor slot. Valid options are: • **F0**—Embedded Service Processor Slot 0 • **F1**—Embedded Service Processor Slot 1 • **FP**—Embedded Service Processor • **R0—**Route Processor Slot 0 • **R1**—Rout Processor Slot 1 • **RP**—Route Processor
service-number	(Optional) Displays information for a dynamically defined service.
access-list	(Optional) Displays WCCP access list information.
cache-info	(Optional) Displays cache-engine information.
interface	(Optional) Displays information about interfaces bound to WCCP services.
statistics	(Optional) Displays internal messaging statistics for WCCP. Displayed counters are self-descriptive.
web-cache	(Optional) Displays information about the web cache service.
web-cache	(Optional) Displays web cache information.
vrf *vrf-identifier*	(Optional) Specifies a virtual routing and forwarding instance (VRF) associated with a service group to display.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. The **vrf** *vrf-identifier* keyword and argument pair was added.

Usage Guidelines

Use the **show platform software wccp** to display global statistics and configuration information related to WCCP on the Cisco ASR 1000 Series Routers. The **show ip wccp** command displays information about software-based (process, fast, and Cisco Express Forwarding [CEF]) forwarding of WCCP packets. The Cisco ASR 1000 Services Routers implement WCCP in hardware, rather than in the CEF or process-switching paths. The **show ip wccp** displays WCCP counters, but only platform fields have nonzero values because redirection happens in hardware.

Examples

The following is sample output from the **show platform software wccp counters** command:

```
Router# show platform software wccp 61 counters

 Service Group (1, 61) counters
        Unassigned count = 0
        Dropped due to closed service count = 0
        Bypass count = 0
        Bypass failed count = 0
        Denied count = 0
        Redirect count = 313635910244
  CE = 10.1.1.2, obj_id = 58, Redirect Packets = 42768533218
  CE = 10.2.1.2, obj_id = 165, Redirect Packets = 45619768766
.
.
.
```

Table 65 describes the significant fields shown in the display.

Table 65 show platform software wccp counters Field Descriptions

Field	Description
Service Group (1, 61) counters	Dynamic service group 61 counters.
Unassigned count	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.
Dropped due to closed service count = 0	This output field is not supported in Cisco IOS XE Release 2.2 and always returns a value of 0.
Bypass count	The number of packets that have been bypassed.
Bypass failed count	Number of bypass packets that WCCP could not find the original input interface.
Denied count	Total number of packets that were not redirected because they did not match the access list.
Redirect count	Total number of packets redirected by the router.
CE = 10.1.1.2, obj_id = 58, Redirect Packets = 42768533218	The number of packets redirected to each cache-engine.

The following is sample output from the **show platform software wccp** *slot* **interface** command:

```
Router# show platform software wccp f0 interface

Interface FastEthernet0/1/0
if_handle: 11, direction: In
Standard web-cache service
```

Table 66 describes the significant fields shown in the display.

Table 66 show platform software wccp slot interface Field Descriptions

Field	Description
Interface FastEthernet0/1/0	Name of the interface on which the WCCP service is applied.
if_handle	The internal interface index associated with the above interface.
direction: In	Specifies if the service is applied inbound or outbound. **Note** WCCP Outbound services are not supported in Cisco IOS XE Release 2.2.
Standard web-cache service	Description of the service which is applied. In this output it is the standard webcache service.

The following is sample output from the **show platform software wccp interface counters** command:

```
Router# show platform software wccp interface counters

 Interface FastEthernet0/1/0
        Input Redirect Packets  = 0
        Output Redirect Packets  = 0
```

Table 67 describes the significant fields shown in the display.

Table 67 show platform software wccp interface counters Field Descriptions

Field	Description
Input Redirect Packets	The number of input packets that have been redirected to the cache engine.
Output Redirect Packets	The number of output packets that have been redirected to the cache engine.

The following is sample output from the **show platform software wccp web-cache counters** command:

```
Router# show platform software wccp web-cache counters

 Service Group (0, 0) counters
        Unassigned count = 0
        Dropped due to closed service count = 0
        Bypass count = 0
        Bypass failed count = 0
        Denied count = 0
        Redirect count = 0
```

Table 68 describes the significant fields shown in the display.

Table 68 show platform software wccp web-cache counters Field Descriptions

Field	Description
Unassigned count	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.
Dropped due to closed service count	Total number of packets that were dropped when WCCP is configured for closed services and an intermediary device is not available to process the service.
Bypass count	The number of packets that have been bypassed.
Bypass failed count	Number of bypass packets that WCCP could not find the original input interface.
Denied count	Total number of packets that were not redirected because they did not match the access list.
Redirect count	Total number of packets redirected by the router.

Related Commands

Command	Description
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.

show sctp association

To display accumulated information for a specific Stream Control Transmission Protocol (SCTP) association, use the **show sctp association** command in privileged EXEC mode.

show sctp association *assoc-id*

Syntax Description

assoc-id	Association identifier, which can be obtained from the output of the **show sctp association list** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command shows only the information that has become available since the last time a **clear sctp statistics** command was executed.

Because thousands of associations can be on a single socket and instance ID, this command has been created to limit the output by displaying the status of one particular association ID.

Examples

The following sample output shows the established associations:

```
Router# show sctp association list

** SCTP Association List **

AssocID: 3011699535, Instance ID: 1
Current state: ESTABLISHED
Local port: 2000, Addrs: 10.1.0.1 10.2.0.1 10.3.0.1 10.0.20.105
Remote port: 1000, Addrs: 10.1.0.1 10.2.0.1 10.3.0.1 10.0.20.105

AssocID: 2740019456, Instance ID: 0
Current state: ESTABLISHED
Local port: 1000, Addrs: 10.1.0.1 10.2.0.1 10.3.0.1 10.0.20.105
Remote port: 2000, Addrs: 10.1.0.1 10.2.0.1 10.3.0.1 10.0.20.105
```

The following sample output shows information for SCTP association 3011699535:

```
Router# show sctp association 3011699535

 AssocID: 3011699535, Instance ID: 1
 Current state: ESTABLISHED
 Local port: 2000, Addrs: 10.1.0.1 10.2.0.1 10.3.0.1 10.0.20.105
 Remote port: 1000, Addrs: 10.1.0.1 10.2.0.1 10.3.0.1 10.0.20.105
```

Table 69 describes the significant fields shown in the display.

Table 69 show sctp association Field Descriptions

Field	Description
AssocID/Instance ID	SCTP association identifier and instance identifier.
Current state	State of SCTP association.
Local port	Port number for the local SCTP endpoint.
Remote port	Port number for the remote SCTP endpoint.
Addrs	IP addresses for the local and remote SCTP endpoints.

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instance	Displays information about SCTP endpoint information for one specific currently configured instance.
show sctp instances	Displays all currently defined SCTP instances.
show sctp statistics	Displays overall statistics counts for SCTP.

show sctp association list

To display identifiers and information for current Stream Control Transmission Protocol (SCTP) associations and instances, use the **show sctp association list** command in privileged EXEC mode.

show sctp association list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **show ip sctp association list** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

Use this command to display the current SCTP association and instance identifiers, the current state of SCTP associations, and the local and remote port numbers and addresses that are used in the associations.

Examples

The following is sample output from this command for three association identifiers:

```
Router# show sctp association list

*** SCTP Association List ****

AssocID:0,  Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8989, Addrs:10.6.0.4 10.5.0.4

AssocID:1,  Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8990, Addrs:10.6.0.4 10.5.0.4

AssocID:2,  Instance ID:0
Current state:ESTABLISHED
Local port:8989, Addrs:10.1.0.2 10.2.0.2
Remote port:8991, Addrs:10.6.0.4 10.5.0.4
```

Table 70 describes the significant fields shown in the display.

Table 70 show sctp association list Field Descriptions

Field	Description
AssocID	SCTP association identifier.
Instance ID	SCTP association instance identifier.
Current state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Local port, Addrs	Port and IP address for the local SCTP endpoint.
Remote port, Addrs	Port and IP address for the remote SCTP endpoint.

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instances	Displays the currently defined SCTP instances.
show sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

show sctp association parameters

To display configured and calculated parameters for the specified Stream Control Transmission Protocol (SCTP) association, use the **show sctp association parameters** command in privileged EXEC mode.

show sctp association parameters *assoc-id*

Syntax Description

assoc-id	Association identifier. Shows the associated ID statistics for the SCTP association.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This commands replaces the **show ip sctp association parameters** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

The **show sctp association parameters** command provides information to determine the stability of SCTP associations, dynamically calculated statistics about destinations, and values to assess network congestion. This command also displays parameter values for the specified association.

This command requires an association identifier. Association identifiers can be obtained from the output of the **show sctp association list** command.

Many parameters are defined for each association. Some are configured parameters, and others are calculated. Three main groupings of parameters are displayed by this command:

- Association configuration parameters
- Destination address parameters
- Association boundary parameters

The association configuration section displays information similar to that in the **show sctp association list** command, including association identifiers, state, and local and remote port and address information. The current primary destination is also displayed.

Examples

The following sample output shows the IP SCTP association parameters for association 0:

```
Router# show sctp association parameters 0

** SCTP Association Parameters **

AssocID: 0  Context: 0  InstanceID: 1
Assoc state: ESTABLISHED  Uptime: 19:05:57.425
Local port: 8181
Local addresses: 10.1.0.3 10.2.0.3

Remote port: 8181
Primary dest addr: 10.5.0.4
Effective primary dest addr: 10.5.0.4
Destination addresses:

10.5.0.4:   State:  ACTIVE
  Heartbeats:  Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/16/38 ms   TOS: 0  MTU: 1500
  cwnd: 5364  ssthresh: 3000  outstand: 768
  Num retrans: 0  Max retrans: 5  Num times failed: 0

10.6.0.4:   State:  ACTIVE
  Heartbeats:  Enabled   Timeout: 30000 ms
  RTO/RTT/SRTT: 1000/4/7 ms   TOS: 0  MTU: 1500
  cwnd: 3960  ssthresh: 3000  outstand: 0
  Num retrans: 0  Max retrans: 5  Num times failed: 0

Local vertag: 9A245CD4  Remote vertag: 2A08D122
Num inbound streams: 10  outbound streams: 10
Max assoc retrans: 5  Max init retrans: 8
CumSack timeout: 200 ms  Bundle timeout: 100 ms
Min RTO: 1000 ms  Max RTO: 60000 ms
LocalRwnd: 18000  Low: 13455   RemoteRwnd: 15252  Low: 13161
Congest levels: 0  current level: 0  high mark: 325
```

Table 71 describes the significant fields shown in the display.

Table 71 show sctp association parameters Field Descriptions

Field	Description
AssocID	SCTP association identifier.
Context	Internal upper-layer handle.
InstanceID	SCTP association instance identifier.
Assoc state	SCTP association state, which can be ESTABLISHED, CLOSED, COOKIE-WAIT, and COOKIE-ECHOED.
Uptime	How long the association has been active.
Local port	Port number for the local SCTP endpoint.
Local addresses	IP addresses for the local SCTP endpoint.
Remote port	Port number for the remote SCTP endpoint.
Primary dest addr	Primary destination address.
Effective primary dest addr	Current primary destination address.
Heartbeats	Status of heartbeats.
Timeout	Heartbeat timeout.

Table 71 show sctp association parameters Field Descriptions (continued)

Field	Description
RTO/RTT/SRTT	Retransmission timeout, round trip time, and smoothed round trip time, calculated from network feedback.
TOS	IP precedence setting.
MTU	Maximum transmission unit size, in bytes, that a particular interface can handle.
cwnd	Congestion window value calculated from network feedback. This value is the maximum amount of data that can be outstanding in the network for that particular destination.
ssthresh	Slow-start threshold value calculated from network feedback.
outstand	Number of outstanding bytes.
Num retrans	Current number of times that data has been retransmitted to that address.
Max retrans	Maximum number of times that data has been retransmitted to that address.
Num times failed	Number of times that the address has been marked as failed.
Local vertag, Remote vertag	Verification tags (vertags). Tags are chosen during association initialization and do not change.
Num inbound streams, Num outbound streams	Maximum inbound and outbound streams. This number does not change.
Max assoc retrans	Maximum association retransmit limit. Number of times that any particular chunk may be retransmitted before a declaration that the association failed, which indicates that the chunk could not be delivered on any address.
Max init retrans	Maximum initial retransmit limit. Number of times that the chunks for initialization may be retransmitted before a declaration that the attempt to establish the association failed.
CumSack timeout	Cumulative selective acknowledge (SACK) timeout. The maximum time that a SACK may be delayed while attempting to bundle together with data chunks.
Bundle timeout	Maximum time that data chunks may be delayed while attempts are made to bundle them with other data chunks.
Min RTO, Max RTO	Minimum and maximum retransmit timeout values allowed for the association.
LocalRwnd, RemoteRwnd	Local and remote receive windows.
Congest levels: current level, high mark	Current congestion level and highest number of packets queued.

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.

Command	Description
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instances	Displays all currently defined SCTP instances.
show sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

show sctp association statistics

To display statistics that have accumulated for the specified Stream Control Transmission Protocol (SCTP) association, use the **show sctp association statistics** command in privileged EXEC mode.

show sctp association statistics *assoc-id*

Syntax Description

assoc-id	Association identifier, which can be obtained from the output of the **show sctp association list** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **show ip sctp association statistics** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command shows only the information that has become available since the last time a **clear sctp statistics** command was executed.

Examples

The following sample output shows the statistics accumulated for SCTP association 0:

```
Router# show sctp association statistics 0

** SCTP Association Statistics **

AssocID/InstanceID: 0/1
Current State: ESTABLISHED
Control Chunks
  Sent: 623874  Rcvd: 660227
Data Chunks Sent
  Total: 14235644  Retransmitted: 60487
  Ordered: 6369678  Unordered: 6371263
  Avg bundled: 18  Total Bytes: 640603980
Data Chunks Rcvd
  Total: 14496585  Discarded: 1755575
  Ordered: 6369741  Unordered: 6371269
  Avg bundled: 18  Total Bytes: 652346325
  Out of Seq TSN: 3069353
```

```
ULP Dgrams
  Sent: 12740941  Ready: 12740961  Rcvd: 12740941
```

Table 69 describes the significant fields shown in the display.

Table 72 show sctp association statistics Field Descriptions

Field	Description
AssocID/InstanceID	SCTP association identifier and instance identifier.
Current State	State of SCTP association.
Control Chunks	SCTP control chunks sent and received.
Data Chunks Sent	SCTP data chunks sent, ordered and unordered.
Data Chunks Rcvd	SCTP data chunks received, ordered and unordered.
ULP Dgrams	Number of datagrams sent, ready, and received by the Upper-Layer Protocol (ULP).

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instances	Displays all currently defined SCTP instances.
show sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.

show sctp errors

To display the error counts logged by the Stream Control Transmission Protocol (SCTP), use the **show sctp errors** command in privileged EXEC mode.

show sctp errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **show ip sctp errors** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command displays all errors across all associations that have been logged since the last time that the SCTP statistics were cleared with the **clear sctp statistics** command. If no errors have been logged, this is indicated in the output.

Examples

The following sample output shows a session with no errors:

```
Router# show sctp errors

*** SCTP Error Statistics ****

No SCTP errors logged.
```

The following sample output shows a session that has SCTP errors:

```
Router# show sctp errors

** SCTP Error Statistics **

Invalid verification tag:       5
Communication Lost:             64
Destination Address Failed:     3
Unknown INIT params rcvd:       16
Invalid cookie signature:       5
Expired cookie:                 1
Peer restarted:                 1
No Listening instance:          2
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show sctp association statistics	Displays the current statistics for the association defined by the association ID.
show sctp instances	Displays the currently defined SCTP instances.
show sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show sctp instance

To display Stream Control Transmission Protocol (SCTP) endpoint information for one specific currently configured instance, use the **show sctp instance** command in user EXEC or privileged EXEC mode.

show sctp instance *instance-id*

Privileged EXEC Mode of Cisco 3845 Series Routers

show sctp instance [**redundancy**] *instance-id*

Syntax Description

instance-id	Instance identifier, which is defined as the transport ID (TransID) value in the output from the **show sockets** command.
redundancy	(Optional) Displays SCTP instance redundancy information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **redundancy** keyword was added on the Cisco 3845 series router.

Usage Guidelines

This command displays information for the currently configured instance with the ID specified in the command syntax. The instance number, local port, and address information are displayed. The instance state is either available or deletion pending. An instance enters the deletion pending state when a request is made to delete it but there are currently established associations for that instance. The instance cannot be deleted immediately and instead enters the pending state. No new associations are allowed in this instance, and when the last association is terminated or fails, the instance is deleted.

The default inbound and outbound stream numbers (see the "Examples" section) are used for establishing incoming associations, the maximum number of associations allowed for this instance is shown, and a snapshot of each existing association is shown, if any exists.

Examples

The following sample output displays information for SCTP instance 0. In this example, instance 0 is using local port 1000 and has three current associations. Field description is self-explanatory.

```
Router# show sctp instance 0

Instance ID:0 Local port:1000 State:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1
  Current associations: (max allowed:200)
  AssocID:0  State:ESTABLISHED  Remote port:8989
```

```
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:1  State:ESTABLISHED  Remote port:8990
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:2  State:ESTABLISHED  Remote port:8991
    Dest addrs:10.6.0.4 10.5.0.4
```

The following sample output displays information for SCTP instance 1. In this example, instance 1 is using local port 9191 and has no current associations. Field description is self-explanatory.

```
Router# show sctp instance 1

Instance ID:1  Local port:9191 State:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1

No current associations established for this instance.
Max allowed:6
```

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show iua as	Displays information about the current condition of an application server.
show iua asp	Displays information about the current condition of an application server process.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp statistics	Displays the overall statistics counts for SCTP.
show sockets	Displays information about sockets.

show sctp instances

To display information for each of the currently configured Stream Control Transmission Protocol (SCTP) instances, use the **show sctp instances** command in privileged EXEC mode.

show sctp instances

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **show ip sctp instances** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command displays information for each of the currently configured instances. The instance number, local port, and address information are displayed. The instance state is either available or deletion pending. An instance enters the deletion pending state when a request is made to delete it but there are currently established associations for that instance. The instance cannot be deleted immediately and instead enters the pending state. No new associations are allowed in this instance, and when the last association is terminated or fails, the instance is deleted.

The default inbound and outbound stream numbers are used for establishing incoming associations, the maximum number of associations allowed for this instance is shown, and a snapshot of each existing association is shown, if any exists.

When you enter the **show sctp instances** command, you must type the complete word **instances** in the command syntax. If you try to enter an abbreviated form of this word, there will be a partial match that identifies the **show sctp instance** *instance-id* command.

Examples

The following sample output shows available IP SCTP instances. In this example, two current instances are active and available. The first is using local port 8989, and the second is using 9191. Instance identifier 0 has three current associations, and instance identifier 1 has no current associations.

```
Router# show sctp instances

*** SCTP Instances ****

Instance ID:0  Local port:8989
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1
  Current associations: (max allowed:6)
  AssocID:0  State:ESTABLISHED  Remote port:8989
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:1  State:ESTABLISHED  Remote port:8990
```

```
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:2  State:ESTABLISHED  Remote port:8991
    Dest addrs:10.6.0.4 10.5.0.4

Instance ID:1  Local port:9191
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1

No current associations established for this instance.
Max allowed:6
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured for the association defined by the association identifier.
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show sctp statistics

To display the overall statistics counts for Stream Control Transmission Protocol (SCTP) activity, use the **show sctp statistics** command in privileged EXEC mode.

show sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced. This command replaces the **show ip sctp statistics** command.
12.4(15)T	This command was moved to the Cisco IOS IP Application Services Command Reference.

Usage Guidelines

This command displays the overall SCTP statistics accumulated since the last **clear sctp statistics** command. It includes numbers for all currently established associations, and for any that have been terminated. The statistics indicated are similar to those shown for individual associations.

Examples

The following sample output shows SCTP statistics:

```
Router# show sctp statistics

*** SCTP Overall Statistics ****

Total Chunks Sent:           2097
Total Chunks Rcvd:           2766

Data Chunks Rcvd In Seq:     538
Data Chunks Rcvd Out of Seq: 0
Total Data Chunks Sent:      538
Total Data Chunks Rcvd:      538
Total Data Bytes Sent:       53800
Total Data Bytes Rcvd:       53800
Total Data Chunks Discarded: 0
Total Data Chunks Retrans:   0

Total SCTP Dgrams Sent:      1561
Total SCTP Dgrams Rcvd:      2228
Total ULP Dgrams Sent:       538
Total ULP Dgrams Ready:      538
Total ULP Dgrams Rcvd:       538
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show sctp association list	Displays a list of all current SCTP associations.
show sctp association parameters	Displays the parameters configured and calculated for the association defined by the association identifier.
show sctp association statistics	Displays the current statistics for the association defined by the association identifier.
show sctp errors	Displays error counts logged by SCTP.
show sctp instances	Displays all currently defined SCTP instances.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show sockets

To display IP socket information, use the **show sockets** command in user EXEC or privileged EXEC mode.

show sockets *process-id* [**detail**] [**events**]

Syntax Description

process-id	Identifier of the IP process to be displayed.
detail	(Optional) Displays detailed information about the selected socket process.
events	(Optional) Displays information about IP socket events.

Command Default

IP socket information is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display the number of sockets currently open and their distribution with respect to the transport protocol process specified by the *process-id* argument.

Use the optional **detail** keyword to display additional information including the local and remote port, protocol type, sub-type for Stream Control Transmission Protocol (SCTP) sockets, IP version, and socket state. Use the optional **events** keyword to display information about the status of the event model for the specified socket. The **events** keyword also displays the events being watched using the event model, events being watched using select calls, and any current events present on the socket.

Use the **show processes** command to display the list of running processes and their associated process IDs.

Examples

The following is sample output from the **show sockets** command when there are no sockets open for the specified process:

```
Router# show sockets 99

There are no open sockets for this process
```

The following example displays the total number of open sockets for the specified process:

```
Router# show sockets 35

Total open sockets - TCP:7, UDP:0, SCTP:0
```

The following example shows how to display detailed information about open sockets:

```
Router# show sockets 35 detail

   FD LPort FPort Proto Type    TransID

   0  5000  0     TCP   STREAM  0x6654DEBC
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   1  5001  0     TCP   STREAM  0x6654E494
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   2  5002  0     TCP   STREAM  0x656710B0
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   3  5003  0     TCP   STREAM  0x65671688
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   4  5004  0     TCP   STREAM  0x65671C60
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   5  5005  0     TCP   STREAM  0x65672238
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   6  5006  0     TCP   STREAM  0x64C7840C
State: SS_ISBOUND
Options: SO_ACCEPTCONN

Total open sockets - TCP:7, UDP:0, SCTP:0
```

The following example displays IP socket event information:

```
Router# show sockets 35 events

Events watched for this process: READ
FD Watched Present Select Present

0 --- --- R-- R--
```

Table 73 describes the significant fields shown in the displays.

Table 73 show sockets Field Descriptions

Field	Description
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination.
LPort	Local TCP port.
FPort	Foreign port.

Table 73 show sockets Field Descriptions (continued)

Field	Description
Proto	Protocol type, such as UDP, TCP, or SCTP.
Type	Type of socket being displayed. Possible socket types include: • STREAM—TCP socket. • DGRAM—UDP socket. • SEQPACKET—SCTP socket.
TransID	Transaction ID number.
State:	Current state of the socket. Possible socket state flags include: • SS_NOFDREF—No file descriptor reference for this socket. • SS_ISCONNECTING—Socket connecting is in progress. • SS_ISBOUND—Socket is bound to TCP. • SS_ISCONNECTED—Socket is connected to peer. • SS_ISDISCONNECTING—Socket disconnecting is in progress. • SS_CANTSENDMORE—Cannot send more data to peer. • SS_CANTRCVMORE—Cannot receive more data from peer. • SS_ISDISCONNECTED—Socket is disconnected. Connection is fully closed.
Options:	Displays socket options. Possible socket options include: • SO_ACCEPTCONN—Socket is accepting a connection. • SO_NBIO—Socket is in a non-blocking I/O mode. • SO_LINGER—Socket waits for a time before all data is sent out.
Events watched for this process:	Details the events that are being watched by the application.
READ	Read events being watched by the application.
Watched	Events being watched by the application.
Present	Watched events that are present on the socket.
Select	Events being watched by the application using the select () call.

Related Commands

Command	Description
clear sockets	Closes all IP sockets and clears the underlying transport connections and data structures.
show ip sctp	Displays information about SCTP.
show processes	Displays information about the active processes.
show udp	Displays IP socket information about UDP processes.

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*]] [**all** | **brief**]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed.
all	(Optional) Displays information for groups that are learned or do not have the **standby ip** command configured.
brief	(Optional) A single line of output summarizes each standby group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The output for the 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(4)T	IPv6 support was added.
12.4(6)T	The output for this command was enhanced to display information about HSRP master and client groups.
12.4(9)T	The output for this command was enhanced to display information about HSRP group shutdown configuration.
12.4(11)T	The output for this command was enhanced to display information about HSRP Bidirectional Forwarding Detection (BFD) peering.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	The output for this command was enhanced to display information about gratuitous ARP packets.
12.4(24)T	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SXI1	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
12.2(33)SRE	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.

Usage Guidelines

To specify a group, you must specify an interface type and number.

Examples

The following is sample output from the **show standby** command:

```
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
  Gratuitous ARP 14 sent, next in 7.412 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
Group name is "HSRP1" (cfgd)
Follow by groups:
    Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.666)
    Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs (next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

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)
  Group 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
  Group name is "hsrp-Et0/2-1" (default)
```

The following is sample output from the **show standby** command with the **brief** keyword specified:

```
Router# show standby brief

Interface   Grp Prio P State    Active addr     Standby addr    Group addr
Et0         0   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, timeout 30 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Et0/1-1" (default)
```

The following is sample output from the **show standby** command when HSRP group shutdown is configured:

```
Router# show standby

Ethernet0/0 - Group 1
State is Init (tracking shutdown)
3 state changes, last state change 00:30:59
Track object 100 state Up
Track object 101 state Down
Track object 103 state Up
```

The following is sample output from the **show standby** command when HSRP BFD peering is enabled:

```
Router# show standby

Ethernet0/0 - Group 2
  State is Listen
    2 state changes, last state change 01:18:18
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 10.0.0.250, priority 120 (expires in 9.396 sec)
  Standby router is 10.0.0.251, priority 110 (expires in 8.672 sec)
    BFD enabled
  Priority 90 (configured 90)
```

```
  Group name is "hsrp-Et0/0-1" (default)
```

The following is sample output from the **show standby** command used to display the state of the standby RP:

```
Router# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

Table 74 describes the significant fields shown in the displays.

Table 74 show standby Field Descriptions

Field	Description
Ethernet - Group	Interface type and number and Hot Standby group number for the interface.
State is	State of local router; can be one of the following: • Active—Indicates the current Hot Standby router. • Standby—Indicates the router next in line to be the Hot Standby router. • Speak—Router is sending packets to claim the active or standby role. • Listen—Router is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak. • 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 **standby ip** command has not been specified. • Init (tracking shutdown)—HSRP groups appear in the Init state when HSRP group shutdown has been configured and a tracked object goes down.
Virtual IP address is, Secondary virtual IP addresses	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 (Address Resolution Protocol) cache entry.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Local virtual MAC address	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 "confgd" (configured).

Table 74 show standby Field Descriptions (continued)

Field	Description
Hello time, hold time	The hello time is the time between hello packets (in seconds) based on the command. The holdtime is the time (in seconds) before other routers declare the active or standby router to be down, based on the **standby timers** command. All routers in an HSRP group use the hello 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 in which the Cisco IOS software will send the next hello packet (in hours:minutes:seconds).
Gratuitous ARP 14 sent, next in 7.412 secs	Number of the gratuitous ARP packet HSRP has sent and the time in seconds when HSRP will send the next gratuitous ARP packet. This output appears only when HSRP sends gratuitous ARP packets.
Authentication	Authentication type configured based on the **standby authentication** command.
key-string	Indicates a key string is used for authentication. Configured key chains are not displayed.
timeout	Duration (in seconds) that 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 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).
BFD enabled	Indicates that BFD peering is enabled on the 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 **standby track** command.
Group name is	The name of the HSRP group.
Follow by groups:	Indicates the client HSRP groups that have been configured to follow this HSRP group.
P	Indicates that the router is configured to preempt.

Related Commands

Command	Description
standby authentication	Configures an authentication string for the HSRP.
standby ip	Activates the HSRP.
standby mac-address	Specifies the virtual MAC address for the virtual router.
standby mac-refresh	Refreshes the MAC cache on the switch by periodically sending packets from the virtual MAC address.

Command	Description
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
standby timers	Configures the time between hello messages and the time before other routers declare the active Hot Standby or standby router to be down.
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.
standby use-bias	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 arp gratuitous

To display the number and configured interval of gratuitous Address Resolution Protocol (ARP) packets sent by Hot Standby Router Protocol (HSRP), use the **show standby arp gratuitous** command in user EXEC or privileged EXEC configuration mode.

show standby arp gratuitous [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Default

The number of user-configured gratuitous ARP packets is not displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays the interface to which HSRP sends gratuitous ARP packets, the interval (in seconds) and the number. Gratuitous ARP packets are sent only when an HSRP group transitions to the Active state.

Examples

The following sample output displays information about HSRP gratuitous ARP packets:

```
Router# show standby arp gratuitous

HSRP Gratuitous ARP
Interface   Interval   Count
Ethernet0/0 3          2
```

Related Commands

Command	Description
debug standby events arp	Displays events related to HSRP.
standby arp gratuitous	Configures the number of gratuitous ARP packets sent by an active HSRP group, and how often they are sent.
standby send arp	Configures HSRP to check that all ARP entries for active HSRP addresses are correct prior to sending gratuitous ARP packets.

show standby capability

To display the limitation on how many virtual MAC addresses that some interfaces can listen to, use the **show standby capability** command in user EXEC or privileged EXEC mode.

show standby capability [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

HSRP allows up to 256 groups to be configured on each interface, but it is possible that the MAC address filter of the interface does not support that many entries. For example, Versatile Interface Processor (VIP) interfaces only support 32 MAC addresses in their MAC address filter. If more HSRP groups are created than there are address filter entries, then it is likely that the router will stop listening to packets sent to the MAC address of an active HSRP group.

Examples

The following is sample output from the **show standby capability** command:

```
Router# show standby capability
7206VXR * indicates hardware may support HSRP
                                                |
Interface          Type                        H  Potential Max Groups
FastEthernet0/0    18  DEC21140A               *  256  (0x60194B00,
0x60194BE8)
FastEthernet1/0    18  DEC21140A               *  256  (0x60194B00,
0x60194BE8)
Ethernet2/0        61  AmdP2                   *  256  (0x601A252C,
0x601A25E4)
Ethernet2/1        61  AmdP2                   *  256  (0x601A252C,
0x601A25E4)
Ethernet2/2        61  AmdP2                   *  256  (0x601A252C,
0x601A25E4)
Ethernet2/3        61  AmdP2                   *  256  (0x601A252C,
0x601A25E4)
Ethernet2/4        61  AmdP2                   *  256  (0x601A252C,
0x601A25E4)
Ethernet2/5        61  AmdP2                   *  256  (0x601A252C,
0x601A25E4)
Ethernet2/6        61  AmdP2                   *  256  (0x601A252C,
```

```
0x601A25E4)
Ethernet2/7         61  AmdP2                *  256  (0x601A252C,
0x601A25E4)
ATM3/0              74  ENHANCED ATM PA      *  256  LAN emulation
TokenRing4/0        66  HAWKEYE              *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/1        66  HAWKEYE              *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/2        66  HAWKEYE              *  3    HSRP TR functional
addresses (0x6076A590)
TokenRing4/3        66  HAWKEYE              *  3    HSRP TR functional
addresses (0x6076A590)
Serial5/0           67  M4T                     -
Serial5/1           67  M4T                     -
Serial5/2           67  M4T                     -
Serial5/3           67  M4T                     -
FastEthernet6/0     18  DEC21140A            *  256  (0x60194B00,
0x60194BE8)
VoIP-Null0          102 VoIP-Null               -
```

Table 75 describes the significant fields in the display.

Table 75 show standby capability Field Descriptions

Field	Description
Interface	Interface type and number for the interface.
Type	Hardware type.
*	Indicates hardware may support HSRP.
Potential Max Groups	An estimate of the number of HSRP groups that a MAC address filter can process for an interface.

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*]

Syntax Description

type number	(Optional) Interface type and number for which output is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show standby delay** command:

```
Router# show standby delay

 Interface          Minimum Reload
 Ethernet0/3        1       5
```

Table 76 describes the significant fields shown in the display.

Table 76 show standby delay Field Descriptions

Field	Description
Interface	Interface type and number.
Minimum	Minimum time (in seconds) to delay HSRP group initialization after an interface comes up.
Reload	Time (in seconds) to delay after the router has reloaded.

Related Commands

Command	Description
standby delay minimum reload	Delays the initialization of HSRP groups.

show standby internal

To display Hot Standby Routing Protocol (HSRP) internal flags and conditions, use the **show standby internal** command in user EXEC or privileged EXEC mode.

show standby internal [*interface-type interface-number* [*group* | **summary** [**all**]] | **summary**]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.
group	(Optional) Group number on the interface for which output is displayed. The range is 0 to 255.
summary	(Optional) Displays the number of configured and learned HSRP groups in various states on the interface.
all	(Optional) Displays HSRP groups on all subinterfaces if the specified interface is the main interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SXI2	This command was modified. The *group* argument and the **summary** and **all** keywords were added.
12.2(33)SRE	This command was modified. The *group* argument and the **summary** and **all** keywords were added.
15.0(1)M	This command was modified. The *group* argument and the **summary** and **all** keywords were added.

Usage Guidelines

The **show standby internal** *interface-type interface-number* **summary** command applies to both the main interface and subinterfaces. When the command is used for the main interface the display output does not include groups on subinterfaces. This command displays all configured and learned HSRP groups in various states on the specified interface or subinterface.

The **show standby internal** *interface-type interface-number* **summary all** command applies only to the main interface, not to subinterfaces. It displays the total number of configured and learned HSRP groups in various states, including groups on all subinterfaces under the main interface.

The **show standby internal summary** command displays all configured and learned HSRP groups in various states on all interfaces.

Examples

The following example shows a configuration example and sample output from the **show standby internal** command for the configuration. The output shows internal flags and hardware and software information for Ethernet interface 2/0. The output shows that HSRP group 1 is configured for priority and preemption, and that the **standby timers** and **standby-use bia** commands have been configured.

```
Router# show standby internal

interface Ethernet2/0
 ip address 10.0.0.254 255.255.0.0
 standby use-bia
 standby version 2
 standby 1 ip 10.0.0.1
 standby 1 timers 2 6
 standby 1 priority 110
 standby 1 preempt

Router# show standby internal

Global           Confg: 0000
Et2/0 If hw      AmdP2, State 0x210040
Et2/0 If hw      Confg: 0001, USEBIA
Et2/0 If hw      Flags: 0000
Et2/0 If sw      Confg: 0040, VERSION
Et2/0 If sw      Flags: 0001, USEBIA
Et2/0 Grp 1      Confg: 0072, IP_PRI, PRIORITY, PREEMPT, TIMERS
Et2/0 Grp 1      Flags: 0000
```

The following sample output from the **show standby internal ethernet0/1 summary all** command shows 400 active configured groups and no active learned groups for Ethernet interface 0/1:

```
Router# show standby internal ethernet 0/1 summary all

               Disable  Init     Learn    Listen   Speak    Standby  Active
Ethernet0/1
Configured     0        0        0        0        0        0        400
Learnt         0        0        0        0        0        0        0
```

Table 77 describes the significant fields shown in the display.

Table 77 show standby internal summary all Field Description

Field	Description
Disable	Number of HSRP groups in the disabled state. An HSRP group that is in the disabled state is not yet ready or able to participate in HSRP. All learned groups are always in the disabled state.
Init	Number of HSRP groups in the initial state. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the Init state.
Learn	Number of HSRP groups in the learned state. A group that is learned is neither in the active nor standby state, nor does it have enough information to attempt to claim the active or standby roles.

Table 77 show standby internal summary all Field Description

Field	Description
Listen	Number of HSRP groups in the listen state. A router in the listen state is neither in the active nor standby state, but if no messages are received from the active or standby router, it will start to speak.
Speak	Number of HSRP groups that are sending packets to claim the active or standby role.
Standby	Number of standby HSRP groups.
Active	Number of active HSRP groups.

Related Commands

Command	Description
show standby	Displays HSRP information.

show standby neighbors

To display information about Hot Standby Router Protocol (HSRP) peer routers on an interface, use the **show standby neighbors** command in privileged EXEC mode.

show standby neighbors [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.

Command Default

HSRP neighbor information is displayed for all interfaces.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display information about HSRP peer neighbors. This command displays the HSRP groups for which each neighbor is acting as the active and standby router and whether Bidirectional Forwarding Detection (BFD) peering is enabled for each neighbor.

Examples

The following example displays the HSRP neighbors on Ethernet interface 0/0. Neighbor 10.0.0.250 is active for group 2 and standby for groups 1 and 8, and is registered with BFD:

```
Router# show standby neighbors Ethernet0/0

HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
    No Active groups
    No Standby groups
    BFD enabled
```

The following example displays information for all HSRP neighbors:

```
Router# show standby neighbors

HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
```

```
    Standby groups: 1
    BFD enabled

HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```

Table 78 describes the significant fields shown in the displays.

Table 78 show standby neighbors Field Descriptions

Field	Description
Active groups	HSRP groups for which an interface is acting as the active peer.
Standby groups	HSRP groups for which an interface is acting as the standby peer.
BFD enabled	Indicates that HSRP BFD peering is enabled.

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
debug standby events neighbor	Displays HSRP neighbor events.
show bfd neighbor	Displays a line-by-line listing of existing BFD adjacencies.
show standby	Displays information about HSRP.
standby bfd	Reenables HSRP BFD peering for a specified interface if it has been disabled.
standby ip	Activates HSRP.

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

ip-address	(Optional) Router IP address.
interface-type interface-number	(Optional) Interface type and number for which output is displayed.
active	(Optional) Active HSRP routers on the subnet.
passive	(Optional) Passive HSRP routers on the subnet.
timers	(Optional) HSRP ICMP redirect timers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following 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 79 describes the significant fields in the display.

Table 79 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.
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 redirect** 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 redirect** 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 redirect** *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
show standby	Displays the HSRP information.
standby redirects	Enables ICMP redirect messages to be sent when HSRP is configured on an interface.

show tcp

To display the status of Transmission Control Protocol (TCP) connections when Cisco IOS or Cisco IOS Software Modularity images re running, use the **show tcp** command in user EXEC or privileged EXEC mode.

show tcp [*line-number*] [**tcb** *address*]

Syntax Description

line-number	(Optional) Absolute line number of the line for which you want to display Telnet connection status.
tcb	(Optional) Specifies the transmission control block (TCB) of the ECN-enabled connection that you want to display.
address	(Optional) TCB hexadecimal address. The valid range is from 0x0 to 0xFFFFFFFF.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The **tcb** keyword and *address* argument were added.
12.4(2)T	The output is enhanced to display status and option flags.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB. The display output was modified to include the SSO capability flag and to indicate the reason that the SSO property failed on a TCP connection.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Examples

Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. To view the appropriate output, choose one of the following sections:

- Cisco IOS Software
- Cisco IOS Software Modularity

Cisco IOS Software

The following is sample output that displays the status and option flags:

```
Router# show tcp
.
```

```
.
.
Status Flags: passive open, active open, retransmission timeout, app closed

Option Flags: vrf id set

IP Precedence value: 6
.
.
.
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
 Status Flags: active open, retransmission timeout
 Option Flags: vrf id set
 IP Precedence value: 6
```

Table 80 contains the types of flags, all possible command output enhancements, and descriptions. See Table 81 through Table 85 for descriptions of the other fields in the sample output.

Table 80 Type of Flags, All Possible Output Enhancements, and Descriptions

Type of Flag	Output Enhancement	Description
Status		
	Passive open	Set if passive open was done.
	Active open	Set if active open was done.
	Retransmission timeout	Set if retransmission timeout aborts.
	Net output pending	Output to network is pending.
	Wait for FIN	Wait for FIN to be acknowledged.
	App closed	Application has closed the TCB.
	Sync listen	Listen and establish a handshake.
	Gen tcbs	TCBs are generated as passive listener.
	Path mtu discovery	Path maximum transmission unit (MTU) discovery is enabled.
	Half closed	TCB is half closed.
	Timestamp echo present	Echo segment is present.
	Stopped reading	Read half is shut down.
Option		
	VRF id set	Set if connection has a VRF table identifier.
	Idle user	Set if the connection is idle.
	Sending urgent data	Set if urgent data is being sent.
	Keepalive running	Set if keepalive timer is running, or if an Explicit Congestion Notification (ECN)-enabled connection, or a TCB address bind is in effect.
	Nagle	Set if performing the Nagle algorithm.
	Always push	All packets and full-sized segments (internal use) are pushed.
	Path mtu capable	Path MTU discovery is configured.

Table 80 Type of Flags, All Possible Output Enhancements, and Descriptions (continued)

Type of Flag	Output Enhancement	Description
	MD5	Message digest 5 (MD) messages are generated.
	Urgent data removed	Urgent data is removed.
	SACK option permitted	Peer permits a selective acknowledgment (SACK) option.
	Timestamp option used	Time-stamp option is in use.
	Reuse local address	Local address can be reused.
	Non-blocking reads	Nonblocking TCP is read.
	Non-blocking writes	Nonblocking TCP is written.
	No delayed ACK	No TCP delayed acknowledgment is sent.
	Win-scale	Peer permits window scaling.
	Linger option set	The linger-on close option is set.

The following is sample output from the **show tcp** command:

```
Router# show tcp

tty0, connection 1 to host cider
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 172.31.232.17, Local port: 11184
Foreign host: 172.31.1.137, Foreign port: 23

Enqueued packets for retransmit: 0, input: 0, saved: 0

Event Timers (current time is 67341276):
Timer:       Retrans   TimeWait    AckHold    SendWnd  KeepAlive
Starts:           30          0         32          0          0
Wakeups:           1          0         14          0          0
Next:              0          0          0          0          0

iss:   67317172  snduna:   67317228  sndnxt:   67317228     sndwnd:   4096
irs: 1064896000  rcvnxt: 1064897597  rcvwnd:       2144  delrcvwnd:      0

SRTT: 317 ms, RTTO: 900 ms, RTV: 133 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 300 ms
Flags: higher precedence, idle user, retransmission timeout
Datagrams (max data segment is 536 bytes):
Rcvd: 41 (out of order: 0), with data: 34, total data bytes: 1596
Sent: 57 (retransmit: 1), with data: 35, total data bytes: 55
```

Table 81 describes the first five lines of output shown in the above display.

Table 81 show tcp Field Descriptions—First Section of Output

Field	Description
tty	Identifying number of the line.
connection	Identifying number of the TCP connection.
to host	Name of the remote host to which the connection has been made.

Table 81 show tcp Field Descriptions—First Section of Output (continued)

Field	Description
Connection state is	A connection progresses through a series of states during its lifetime. The states that follow are shown in the order in which a connection progresses through them. • LISTEN—Waiting for a connection request from any remote TCP and port. • SYNSENT—Waiting for a matching connection request after having sent a connection request. • SYNRCVD—Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB—Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1—Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent. • FINWAIT2—Waiting for a connection termination request from the remote TCP host. • CLOSEWAIT—Waiting for a connection termination request from the local user. • CLOSING—Waiting for a connection termination request acknowledgment from the remote TCP host. • LASTACK—Waiting for an acknowledgment of the connection termination request previously sent to the remote TCP host. • TIMEWAIT—Waiting for enough time to pass to be sure that the remote TCP host has received the acknowledgment of its connection termination request. • CLOSED—Indicates no connection state at all. • For more information about TCBs, see RFC 793, *Transmission Control Protocol Functional Specification.*
I/O status	Number that describes the current internal status of the connection.
unread input bytes	Number of bytes that the lower-level TCP processes have read but that the higher-level TCP processes have not yet processed.
Local host	IP address of the network server.
Local port	Local port number, as derived from the following equation: *line-number* + (512 * *random-number*). (The line number uses the lower nine bits; the other bits are random.)
Foreign host	IP address of the remote host to which the TCP connection has been made.
Foreign port	Destination port for the remote host.

Table 81 show tcp Field Descriptions—First Section of Output (continued)

Field	Description
Enqueued packets for retransmit	Number of packets that are waiting on the retransmit queue. These are packets on this TCP connection that have been sent but that have not yet been acknowledged by the remote TCP host.
input	Number of packets that are waiting on the input queue to be read by the user.
saved	Number of received out-of-order packets that are waiting for all packets in the datagram to be received before they enter the input queue. For example, if packets 1, 2, 4, 5, and 6 have been received, packets 1 and 2 would enter the input queue, and packets 4, 5, and 6 would enter the saved queue.

Note Use the **show tcp brief** command to display information about the ECN-enabled connections.

The following line of output shows the current elapsed time according to the system clock of the local host. The time shown is the number of milliseconds since the system started.

```
Event Timers (current time is 67341276):
```

The following lines of output display the number of times that various local TCP timeout values were reached during this connection. In this example, the local host re-sent data 30 times because it received no response from the remote host, and it sent an acknowledgment many more times because there was no data.

```
Timer:        Retrans    TimeWait     AckHold     SendWnd     Keepalive     GiveUp     PmtuAger
Starts:            30           0          32           0             0          0            0
Wakeups:            1           0          14           0             0          0            0
Next:               0           0           0           0             0          0            0
```

Table 82 describes the fields in the above lines of output.

Table 82 show tcp Field Descriptions—Second Section of Output

Field	Description
Timer	Names of the timer types in the output.
Starts	Number of times that the timer has been triggered during this connection.
Wakeups	Number of keepalives sent without receiving any response. (This field is reset to zero when a response is received.)
Next	System clock setting that triggers a timer for the next time an event (for example, TimeWait, AckHold, SendWnd, etc.) occurs.
Retrans	Retransmission timer is used to time TCP packets that have not been acknowledged and that are waiting for retransmission.
TimeWait	A time-wait timer ensures that the remote system receives a request to disconnect a session.
AckHold	An acknowledgment timer delays the sending of acknowledgments to the remote TCP in an attempt to reduce network use.

Table 82 show tcp Field Descriptions—Second Section of Output (continued)

Field	Description
SendWnd	A send-window timer ensures that there is no closed window due to a lost TCP acknowledgment.
KeepAlive	A keepalive timer controls the transmission of test messages to the remote device to ensure that the link has not been broken without the knowledge of the local device.
GiveUp	A give-up timer determines the amount of time a local host will wait for an acknowledgment (or other appropriate reply) of a transmitted message after the the maximum number of retransmissions has been reached. If the timer expires, the local host gives up retransmission attempts and declares the connection dead.
PmtuAger	A path MTU (PMTU) age timer is an interval that displays how often TCP estimates the PMTU with a larger maximum segment size (MSS). When the age timer is used, TCP path MTU becomes a dynamic process. If the MSS is smaller than what the peer connection can manage, a larger MSS is tried every time the age timer expires. The discovery process stops when the send MSS is as large as the peer negotiated or the timer has been manually disabled by being set to infinite.

The following lines of output display the sequence numbers that TCP uses to ensure sequenced, reliable transport of data. The local host and remote host each use these sequence numbers for flow control and to acknowledge receipt of datagrams.

```
iss:   67317172  snduna:   67317228  sndnxt:   67317228     sndwnd:   4096
irs: 1064896000  rcvnxt: 1064897597  rcvwnd:       2144  delrcvwnd:      0
```

Table 83 describes the fields shown in the display above.

Table 83 show tcp Field Descriptions—Sequence Numbers

Field	Description
iss	Initial send sequence number.
snduna	Last send sequence number that the local host sent but for which it has not received an acknowledgment.
sndnxt	Sequence number that the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number that the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrcvwnd	Delayed receive window—data that the local host has read from the connection but has not yet subtracted from the receive window that the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.

The following lines of output display values that the local host uses to keep track of transmission times so that TCP can adjust to the network that it is using.

```
SRTT: 317 ms, RTTO: 900 ms, RTV: 133 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 300 ms
Flags: higher precedence, idle user, retransmission timeout
```

Table 84 describes the significant fields shown in the output above.

Table 84 show tcp Field Descriptions—Line Beginning with "SRTT"

Field	Description
SRTT	A calculated smoothed round-trip timeout.
RTTO	Round-trip timeout.
RTV	Variance of the round-trip time.
KRTT	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT	Largest recorded round-trip timeout.
ACK hold	Time for which the local host will delay an acknowledgment in order to add data to it.
Flags	Properties of the connection.

Note For more information on the above fields, see *Round Trip Time Estimation*, P. Karn and C. Partridge, ACM SIGCOMM-87, August 1987.

The following lines of output display the number of datagrams that are transported with data.

```
Datagrams (max data segment is 536 bytes):
Rcvd: 41 (out of order: 0), with data: 34, total data bytes: 1596
Sent: 57 (retransmit: 1), with data: 35, total data bytes: 55
```

Table 85 describes the significant fields shown in the last lines of the **show tcp** command output.

Table 85 show tcp Field Descriptions—Last Section of Output

Field	Description
Rcvd	Number of datagrams that the local host has received during this connection (and the number of these datagrams that were out of order).
with data	Number of these datagrams that contained data.
total data bytes	Total number of bytes of data in these datagrams.
Sent	Number of datagrams that the local host sent during this connection (and the number of these datagrams that needed to be re-sent).
with data	Number of these datagrams that contained data.
total data bytes	Total number of bytes of data in these datagrams.

The following is sample output from the **show tcp tcb** command that displays detailed information by hexadecimal address about an ECN-enabled connection:

```
Router# show tcp tcb 0x62CD2BB8

Connection state is LISTEN, I/O status: 1, unread input bytes: 0
Connection is ECN enabled
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 12000

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x4F31940):
Timer          Starts    Wakeups            Next
Retrans             0          0             0x0
TimeWait            0          0             0x0
AckHold             0          0             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:          0 snduna:          0 sndnxt:          0     sndwnd:      0
irs:          0 rcvnxt:          0 rcvwnd:       4128  delrcvwnd:      0

SRTT: 0 ms, RTTO: 2000 ms, RTV: 2000 ms, KRTT: 0 ms
minRTT: 60000 ms, maxRTT: 0 ms, ACK hold: 200 ms
Flags: passive open, higher precedence, retransmission timeout

TCB is waiting for TCP Process (67)

Datagrams (max data segment is 516 bytes):
Rcvd: 6 (out of order: 0), with data: 0, total data bytes: 0
Sent: 0 (retransmit: 0, fastretransmit: 0), with data: 0, total data
bytes: 0
```

Cisco IOS Software Modularity

The following is sample output from the **show tcp tcb** command from a Software Modularity image:

```
Router# show tcp tcb 0x1059C10

Connection state is ESTAB, I/O status: 0, unread input bytes: 0
Local host: 10.4.2.32, Local port: 23
Foreign host: 10.4.2.39, Foreign port: 11000
VRF table id is: 0

Current send queue size: 0 (max 65536)
Current receive queue size: 0 (max 32768)  mis-ordered: 0 bytes

Event Timers (current time is 0xB9ACB9):
Timer          Starts    Wakeups            Next(msec)
Retrans             6          0                 0
SendWnd             0          0                 0
TimeWait            0          0                 0
AckHold             8          4                 0
KeepAlive          11          0           7199992
PmtuAger            0          0                 0
GiveUp              0          0                 0
Throttle            0          0                 0
```

```
irs:    1633857851  rcvnxt: 1633857890  rcvadv: 1633890620  rcvwnd:  32730
iss:    4231531315  snduna: 4231531392  sndnxt: 4231531392  sndwnd:   4052
sndmax: 4231531392  sndcwnd:     10220

SRTT: 84 ms,  RTTO: 650 ms,  RTV: 69 ms,  KRTT: 0 ms
minRTT: 0 ms,  maxRTT: 200 ms, ACK hold: 200 ms

Keepalive time: 7200 sec, SYN wait time: 75 sec
Giveup time: 0 ms, Retransmission retries: 0, Retransmit forever: FALSE

State flags: none

Feature flags: Nagle

Request flags: none
Window scales: rcv 0, snd 0, request rcv 0, request snd 0
Timestamp option: recent 0, recent age 0, last ACK sent          0

Datagrams (in bytes): MSS 1460, peer MSS 1460, min MSS 1460, max MSS 1460
Rcvd: 14 (out of order: 0), with data: 10, total data bytes: 38
Sent: 10 (retransmit: 0, fastretransmit: 0), with data: 5, total data bytes: 76

Header prediction hit rate: 72 %

Socket states: SS_ISCONNECTED, SS_PRIV

Read buffer flags: SB_WAIT, SB_SEL, SB_DEL_WAKEUP
Read notifications: 4

Write buffer flags: SB_DEL_WAKEUP
Write notifications: 0
Socket status: 0
```

Related Commands

Command	Description
show tcp brief	Displays a concise description of TCP connection endpoints.

show tcp brief

To display a concise description of TCP connection endpoints, use the **show tcp brief** command in user EXEC or privileged EXEC mode.

show tcp brief [**all** | **numeric**]

Syntax Description

all	(Optional) Displays status for all endpoints in Domain Name System (DNS) hostname format. Without this keyword, endpoints in the LISTEN state are not shown.
numeric	(Optional) Displays status for all endpoints in IP format.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.4(2)T	The **numeric** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

If the **ip domain lookup** command is enabled on the router, and you execute the **show tcp brief** command, the response time of the router to display the output is very slow. To get a faster response, you should disable the **ip domain lookup** command.

Examples

The following is sample output from the **show tcp brief** command while a user is connected to the system by using Telnet:

```
Router# show tcp brief

TCB       Local Address           Foreign Address        (state)
609789AC  Router.cisco.com.23     cider.cisco.com.3733   ESTAB
```

The following example shows the IP activity by using the **numeric** keyword to display the addresses in IP format:

```
Router# show tcp brief numeric

TCB           Local Address          Foreign Address     (state)
6523A4FC      10.1.25.3.11000        10.1.25.3.23         ESTAB
65239A84      10.1.25.3.23           10.1.25.3.11000      ESTAB
```

```
653FCBBC      *.1723 *.* LISTEN
```

Table 86 describes the significant fields shown in the display.

Table 86 show tcp brief Field Descriptions

Field	Description
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	The state of the connection. States are described in the syntax description of the **show tcp** command.

Related Commands

Command	Description
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
show tcp	Displays the status of TCP connections.

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.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4, and the output was modified to display Software Modularity information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Cisco IOS Software Modularity

There are three transport protocols used in Software Modularity: TCP, UDP, and raw IP. The transport protocol statistics are generally counters, though some are averages and time stamps. Use the **show tcp statistics** command to display the TCP statistics and use the **clear tcp statistics** command to reset the TCP statistics. Many of the statistics are relevant to all of the transport protocols. To view the other transport protocol statistics used in Software Modularity, see the **show raw statistics** and **show udp statistics** commands.

Examples

Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images. To view the appropriate output, choose one of the following sections:

- Cisco IOS Software
- Cisco IOS Software Modularity

Cisco IOS Software

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 87 describes the significant fields shown in the display.

Table 87 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.
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 unsent 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.

Table 87 show tcp statistics Field Descriptions (continued)

Field	Description
connections accepted	Number of connections accepted.
connections established	Number of connections established.
Connections closed	Number of connections closed.
Total rxmt timeout	Number of times that 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.

Cisco IOS Software Modularity

The following is sample output from the **show tcp statistics** command when a Software Modularity image is running under Cisco IOS Release 12.2(18)SXF4:

```
Router# show tcp statistics

Current packet level is 0 (Clear)
Rcvd: 0 Total, 0 no port
      0 checksum error, 0 bad offset, 0 too short
      0 packets (0 bytes) in sequence
      0 dup packets (0 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 for unsent data
      0 ack packets (0 bytes)
      0 packets dropped due to PAWS
      0 packets dropped due to receive packet limits
      0 packets dropped due to receive byte limits
Sent: 0 Total, 0 urgent packets
      0 control packets (including 0 retransmitted)
      0 data packets (0 bytes)
      0 data packets (0 bytes) retransmitted
      0 data packets (0 bytes) fastretransmitted
      0 Sack retransmitted bytes, 0 Sack skipped bytes
      0 ack only packets (0 delayed)
      0 window probe packets, 0 window update packets
0 Connections initiated, 0 connections accepted, 0 connections established
0 Connections closed (including 0 dropped, 0 embryonic dropped)
0 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 RTO, 0 KRTO (milliseconds)
0 VJ SRTT, 0 variance (milliseconds)
0 min RTT, 0 max RTT (milliseconds)
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
0 increase MSS, 0 decrease MSS
15 Open sockets
0 Timer interrupts
0 Packets used by socket I/O
0 Packets used by TCP reassembly
0 Packets recovered after starvation
```

```
0 Packet memory warnings
0 Packet memory alarms
0 Packet allocation errors
0 Packet to octet switches due to send flow control
0 Packet to octet switches due to partial ACKs
0 Packet to octet switches due to inadequate resources
0 Output function calls
0 Truncated write I/O vectors
0 Transmission pulse errors
0 Packet punts from IP 0 Packet punts to IP
0 Packet punts from application
0 Packet punts to application
```

Table 88 describes the significant fields shown in the display that are different from Table 87 on page 514.

Table 88 show tcp statistics (Software Modularity) Field Descriptions

Field	Description
Current packet level	A packet level of 0 (Clear) shows that less than 67 percent of the packet supply is in use. A packet level of 1 (Warn) shows that at least 67 percent of the packet supply is in use, and a packet level of 2 (Alarm) shows that at least 90 percent of the packet supply is in use.
packets dropped due to PAWS	Number of packets dropped because of sequence number wrap-around on high speed, low latency networks.
packets dropped due to receive packet limits	Number of packets dropped after the receive packet limit is exceeded.
packets dropped due to receive byte limits	Number of packets dropped after the receive byte limit is exceeded.
data packets fastretransmitted	Number of packets retransmitted before timer expiry because of excessive duplicate ACKs.
Sack retransmitted bytes, Sack skipped bytes	Number of retransmitted bytes due to selective acknowledgement.
RTO, KRTO	RTO is the current retransmission timeout, as calculated by Van Jacobson's algorithm. KRTO is the exponentially backed off retransmission timeout.
VJ SRTT, variance	Scaled mean and variance round trip times used by Van Jacobson's algorithm.
min RTT, max RTT	Minimum and maximum round-trip time (RTT), in milliseconds.
increase MSS, decrease MSS	Number of times that the maximum segment size (MSS) changed because of path MTU discovery.
Open sockets	Number of open sockets.
Timer interrupts	Number of packets received with timer interrupts.
Packets used by socket I/O	Number of packets enqueued on socket send buffers, receive buffers, or reassembly queues. In summary, the number of packets currently being held by the transport protocol.
Packets used by TCP reassembly	Number of out of order segments that cannot be passed to application because of missing holes in the data stream. These holes will be filled when the peer retransmits.

Table 88 show tcp statistics (Software Modularity) Field Descriptions (continued)

Field	Description
Packets recovered after starvation	Number of packets released by the transport protocol due to memory warnings or memory alarms.
Packet memory warnings	Number of packets with memory warnings.
Packet memory alarms	Number of packets with memory alarms.
Packet allocation errors	Number of packets with allocation errors.
Packet to octet switches due to send flow control	Number of times that TCP switched from packet I/O to octet buffer I/O because of inadequate send window.
Packet to octet switches due to partial ACKs	Number of times that TCP switched from packet I/O to octet buffer I/O because of partially acknowledged data.
Packet to octet switches due to inadequate resources	Number of times that TCP switched from packet I/O to octet buffer I/O because of inadequate packet resources.
Output function calls	Number of times that the TCP output engine was invoked.
Truncated write I/O vectors	Number of truncated segments due to inadequate write buffers.
Transmission pulse errors	Number of transmission signaling mechanism errors.
Packet punts from IP, Packet punts to IP	Number of batches of packets moved from and to the IP layer.
Packet punts from application, Packet punts to application	Number of batches of packets moved from and to the application layers.

Related Commands

Command	Description
clear tcp statistics	Clears TCP statistics.
show raw statistics	Displays raw IP transport protocol statistics.
show udp statistics	Displays UDP transport protocol statistics.

show tech-support

To display general information about the router when it reports a problem, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**page**] [**password**] [**cef** | **ipc** | **ipmulticast** [**vrf** *vrf-name*] | **isis** | **mpls** | **ospf** [*process-id* | **detail**] | **rsvp** | **voice** | **wccp**]

Cisco 7600 Series

show tech-support [**cef** | **ipmulticast** [**vrf** *vrf-name*] | **isis** | **password** [**page**] | **platform** | **page** | **rsvp**]

Syntax Description

page	(Optional) Causes the output to display a page of information at a time.
password	(Optional) Leaves passwords and other security information in the output.
cef	(Optional) Displays **show** command output specific to Cisco Express Forwarding.
ipc	(Optional) Displays **show** command output specific to Inter-Process Communication (IPC).
ipmulticast	(Optional) Displays **show** command output related to the IP Multicast configuration, including Protocol Independent Multicast (PIM) information, Internet Group Management Protocol (IGMP) information, and Distance Vector Multicast Routing Protocol (DVMRP) information.
vrf *vrf-name*	(Optional) Specifies a multicast Virtual Private Network (VPN) routing and forwarding instance (VRF).
isis	(Optional) Displays **show** command output specific to Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System Protocol (IS-IS).
mpls	(Optional) Displays **show** command output specific to Multiprotocol Label Switching (MPLS) forwarding and applications.
ospf [*process-id* | **detail**]	(Optional) Displays **show** command output specific to Open Shortest Path First Protocol (OSPF) networking.
rsvp	(Optional) Displays **show** command output specific to Resource Reservation Protocol (RSVP) networking.
voice	(Optional) Displays **show** command output specific to voice networking.
wccp	(Optional) Displays **show** command output specific to Web Cache Communication Protocol (WCCP).
platform	(Optional) Displays platform-specific **show** command output.

Defaults

The output scrolls without page breaks.
Passwords and other security information are removed from the output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
11.3(7), 11.2(16)	The output for this command was expanded to show additional information for **boot**, **bootflash**, **context**, and **traffic** for all enabled protocols.
12.0	The output for this command was expanded to show additional information for **boot**, **bootflash**, **context**, and **traffic** for all enabled protocols. The **cef**, **ipmulticast**, **isis**, **mlps**, and **ospf** keywords were added to this command.
12.2(13)T	Support for AppleTalk EIGRP, Apollo Domain, Banyan VINES, Novell Link-State Protocol, and XNS was removed from Cisco IOS software.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.3(4)T	The output of this command was expanded to include the output from the **show inventory** command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(30)S	The **show tech-support ipmulticast** command was changed as follows: • Support for bidirectional PIM and Multicast VPN (MVPN) was added. • The **vrf** *vrf-name* option was added. The output of the **show tech-support ipmulticast** command (without the **vrf** *vrf-name* keyword and argument) was changed to include the output from these commands: • **show ip pim int df** • **show ip pim mdt** • **show ip pim mdt bgp** • **show ip pim rp metric**
12.3(16)	This command was integrated into Cisco IOS Release 12.3(16).
12.2(18)SXF	The **show tech-support ipmulticast** command was changed as follows: • Support for bidirectional PIM and MVPN was added. • The **vrf** *vrf-name* option was added. The output of the **show tech-support ipmulticast vrf** command was changed to include the output from these commands: • **show mls ip multicast rp-mapping gm-cache** • **show mmls gc process** • **show mmls msc rpdf-cache** The output of the **show tech-support ipmulticast** command (without the **vrf** *vrf-name* keyword and argument) was changed to include the output from these commands: • **show ip pim int df** • **show ip pim mdt** • **show ip pim mdt bgp** • **show ip pim rp metric** Support to interrupt and terminate the **show tech-support** output was added.

Release	Modification
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.4(7)	This command was integrated into Cisco IOS Release 12.4(7).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The output of this command was expanded to include partial **show dmvpn details** command output.
15.0(1)M	This command was modified. The **wccp** and **voice** keywords were added.
12.2(33)SRE	This command was modified. The **wccp** keyword was added.
Cisco IOS XE Release 2.5	This command was modified. The **wccp** keyword was added.

Usage Guidelines

To interrupt and terminate the **show tech-support** output, simultaneously press and release the **CTRL**, **ALT**, and **6** keys.

Press the **Return** key to display the next line of output, or press the **Spacebar** to display the next page of information. If you do not enter the **page** keyword, the output scrolls (that is, it does not stop for page breaks).

If you do not enter the **password** keyword, passwords and other security-sensitive information in the output are replaced with the label "<removed>."

The **show tech-support** command is useful for collecting a large amount of information about your routing device for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.



Note This command can generate a very large amount of output. You may want to redirect the output to a file using the **show inventory | redirect** *url* command syntax extension. Redirecting the output to a file also makes sending this output to your technical support representative easier. See the command documentation for **show <command> | redirect** for more information on this option.

The **show tech-support** command displays the output of a number of **show** commands at once. The output from this command varies depending on your platform and configuration. For example, access servers display voice-related **show** command output. Additionally, the **show** *protocol* **traffic** commands are displayed for only the protocols enabled on your device. For a sample display of the output of the **show tech-support** command, see the individual **show** command listed.

If you enter the **show tech-support** command without arguments, the output displays, but is not limited to, the equivalent of these **show** commands:

- **show appletalk traffic**
- **show bootflash**
- **show bootvar**
- **show buffers**
- **show cdp neighbors**
- **show cef**
- **show clns traffic**
- **show context**
- **show controllers**

- **show decnet traffic**
- **show disk0: all**
- **show dmvpn details**
- **show environment**
- **show fabric channel-counters**
- **show file systems**
- **show interfaces**
- **show interfaces switchport**
- **show interfaces trunk**
- **show ip interface**
- **show ip traffic**
- **show logging**
- **show mac-address-table**
- **show module**
- **show power**
- **show processes cpu**
- **show processes memory**
- **show running-config**
- **show spanning-tree**
- **show stacks**
- **show version**
- **show vlan**

Note Crypto information is not duplicated by the **show dmvpn details** command output.

When the **show tech-support** command is entered on a virtual switch (VS), the output displays the output of the **show module** command and the **show power** command for both the active and standby switches.

Use of the optional **cef**, **ipc**, **ipmulticast**, **isis**, **mpls**, **ospf**, or **rsvp** keywords provides a way to display a number of **show** commands specific to a particular protocol or process in addition to the **show** commands listed previously.

For example, if your Technical Assistance Center (TAC) support representative suspects that you may have a problem in your Cisco Express Forwarding (CEF) configuration, you may be asked to provide the output of the **show tech-support cef** command. The **show tech-support** [**page**] [**password**] **cef** command will display the output from the following commands in addition to the output for the standard **show tech-support** command:

- **show adjacency summary**
- **show cef drop**
- **show cef events**
- **show cef interface**

- **show cef not-cef-switched**
- **show cef timers**
- **show interfaces stats**
- **show ip cef events summary**
- **show ip cef inconsistency records detail**
- **show ip cef summary**

If you enter the **ipmulticast** keyword, the output displays, but is not limited to, these **show** commands:

- **show ip dvmrp route**
- **show ip igmp groups**
- **show ip igmp interface**
- **show ip mcache**
- **show ip mroute**
- **show ip mroute count**
- **show ip pim interface**
- **show ip pim interface count**
- **show ip pim interface df**
- **show ip pim mdt**
- **show ip pim mdt bgp**
- **show ip pim neighbor**
- **show ip pim rp**
- **show ip pim rp metric**
- **show mls ip multicast rp-mapping gm-cache**
- **show mmls gc process**
- **show mmls msc rpdf-cache**

If you enter the **wccp** keyword, the output displays, but is not limited to, these **show** commands:

- **show ip wccp** *service-number*
- **show ip wccp interfaces cef**

Examples

For a sample display of the output from the **show tech-support** command, refer to the documentation for the **show** commands listed in the "Usage Guidelines" section.

Related Commands

Command	Description
dir	Displays a list of files on a file system.
show appletalk traffic	Displays statistics about AppleTalk traffic, including MAC IP traffic.
show bootflash	Displays the contents of boot flash memory.

Command	Description
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show buffers	Displays statistics for the buffer pools on the network server.
show cdp neighbors	Displays detailed information about neighboring devices discovered using Cisco Discovery Protocol.
show cef	Displays information about packets forwarded by Cisco Express Forwarding.
show clns traffic	Displays a list of the CLNS packets this router has seen.
show <*command*> **| redirect**	Redirects the output of any **show** command to a file.
show context	Displays context data.
show controllers	Displays information that is specific to the hardware.
show controllers tech-support	Displays general information about a VIP card for problem reporting.
show decnet traffic	Displays the DECnet traffic statistics (including datagrams sent, received, and forwarded).
show disk:0	Displays flash or file system information for a disk located in slot 0:
show dmvpn details	Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.
show environment	Displays temperature, voltage, and blower information on the Cisco 7000 series routers, Cisco 7200 series routers, Cisco 7500 series routers, Cisco 7600 series routers, Cisco AS5300 series access servers, and the Gigabit Switch Router.
show fabric channel counters	Displays the fabric channel counters for a module.
show file system	Lists available file systems.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
show interfaces trunk	Displays the interface-trunk information.
show inventory	Displays the product inventory listing and UDI of all Cisco products installed in the networking device.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip traffic	Displays statistics about IP traffic.
show ip wccp	Displays global statistics related to WCCP.
show logging	Displays the state of syslog and the contents of the standard system logging buffer.
show mac-address table	Displays the MAC address table.
show module	Displays module status and information.
show power	Displays the current power status of system components.
show processes cpu	Displays information about the active processes.
show processes memory	Displays the amount of memory used.

Command	Description
show running-config	Displays the current configuration of your routing device.
show spanning-tree	Displays information about the spanning tree state.
show stacks	Displays the stack usage of processes and interrupt routines.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
show vlan	Displays VLAN information.

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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
```

Table 89 describes the significant fields shown in the display.

Table 89 show time-range ipc Field Descriptions

Field	Description
RP Time range Updates Sent	Number of time-range updates sent by the Route Processor.
RP Time range Deletes Sent	Number of time-range deletes sent by the Route Processor.

Related Commands

Command	Description
clear time-range ipc	Clears the time-range IPC message statistics and counters between the Route Processor and the line card.
debug time-range ipc	Enables debugging output for monitoring the time-range IPC messages between the Route Processor and the line card.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track [*object-number* [**brief**] | **interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

Syntax Description

object-number	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP-route objects.
resolution	(Optional) Displays resolution of tracked parameters.
timers	(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.
12.4(2)T	The output was enhanced to display stub objects.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	This command was enhanced to display information about the status of an interface when carrier-delay detection has been enabled.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(20)T	The output was enhanced to display IP SLAs information.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

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
```

The following example shows the state of the IP SLAs tracking:

```
Router# show track 50

Track 50
  IP SLA 400 state
  State is Up
    1 change, last change 00:00:23
  Delay up 60 secs, down 30 secs
  Latest operation return code: Unknown
```

The following example shows whether a route is reachable:

```
Router# show track 3

Track 3
   IP SLA 1 reachability
   Reachability is Up
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
   Tracked by:
     HSRP Ethernet0/1 3
```

Table 90 describes the significant fields shown in the displays.

Table 90 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet0/2 ip routing	Interface type, interface number, and object that is being 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 that 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, in seconds, 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 91 describes the significant fields shown in the displays.

Table 91 show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Boolean AND is Down	Each object defined in the list must be in a down state.
1 change, last change	Number of times that 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.

The following example shows information about a stub object that has been created to be tracked using Embedded Event Manager (EEM):

```
Router# show track

Track 1
  Stub-object
  State is Up
    1 change, last change 00:00:04, by Undefined
```

The following example shows information about a stub object when the **brief** keyword is used:

```
Router# show track brief

Track   Object                          Parameter        Value Last Change
1       Stub-object Undefined                            Up    00:00:12
```

The following example shows information about the line-protocol state on an interface that is being tracked and which has carrier-delay detection enabled:

```
Router# show track

Track 101
Interface Ethernet1/0 line-protocol
Line protocol is Down (carrier-delay)
1 change, last change 00:00:03
```

Table 92 describes the significant fields shown in the displays.

Table 92 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface Ethernet1/0 line-protocol	Interface type, interface number, and object that is being tracked.
Line protocol is Down (carrier-delay)	State of the interface with the carrier-delay parameter taken into consideration.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Table 93 describes the significant fields shown in the displays.

Table 93 show track brief Field Descriptions

Field	Description
Track	Object number that is being tracked.
Object	Definition of stub object.
Parameter	Tracking parameters.
Value	State value of the object, displayed as Up or Down.
last change	Time (in *hh:mm:ss*) since the state of a tracked object last changed.

Related Commands

Command	Description
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

show udp

To display IP socket information about User Datagram Protocol (UDP) processes, use the **show udp** command in user EXEC or privileged EXEC mode.

show udp [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about the selected socket process.

Command Default

IP socket information about UDP processes is not displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to verify that the UDP 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 udp** command with the **detail** keyword specified:

```
Router# show udp detail

 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  67    0  0   2211 0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  2517  0   0  11   0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5000  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5001  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5002  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5003  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
```

```
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
17       10.0.0.0    0         10.0.21.70  5004  0  0   211  0
Queues: output 0
        input  0 (drops 0, max 50, highwater 0)
```

Table 94 describes the significant fields shown in the display.

Table 94 show udp Field Descriptions

Field	Description
Proto	Protocol type, such as UDP, TCP, or SCTP.
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.
Local	Local address. If the local address is considered illegal or is the address 0.0.0.0, “--any--” is displayed.
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.

Related Commands

Command	Description
clear sockets	Closes all IP sockets and clears the underlying transport connections and data structures.
show ip sctp	Displays information about SCTP.
show processes	Displays information about the active processes.
show sockets	Displays IP socket information.

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 [**all** | **brief**]

Syntax Description

all	(Optional) Provides VRRP group information about all VRRP groups, including groups in a disabled state.
brief	(Optional) Provides a summary view of the group information.

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(14)T	This command was enhanced to display message digest algorithm 5 (MD5) authentication for a VRRP using text strings, key chains, or key strings.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was enhanced to display synchronized state information from the active route processor (RP).
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.
Cisco IOS XE Release 2.6	This command was modified. The output was modified to display information about configured Virtual Router Redundancy Service (VRRS) names.

Usage Guidelines

If no group is specified, the status for all groups is displayed.

Examples

The following is sample output from 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
```

The following sample output shows the MD5 authentication for a VRRP group using a key string:

```
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
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
```

The following is sample output from the **show vrrp** command in Cisco IOS Release 12.2(33)SRC or later releases, displaying peer RP state information:

```
Router# show vrrp

Ethernet0/0 - Group 1
  State is Init (standby RP, peer state is Master)
  Virtual IP address is 172.24.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 255
  Master Router is 172.24.1.1 (local), priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.003 sec
```

The following sample output displays information about a configured VRRS group name:

```
Router# show vrrp

 Gige0/0/0 - Group 1
State is Master
```

```
Virtual IP address is 10.0.0.7
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 100
VRRS Group name CLUSTER1 ! Configured VRRS Group Name
Master Router is 10.0.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

Table 95 describes the significant fields shown in the displays.

Table 95 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).
(standby RP, peer state is Master)	State of the peer RP.
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 **vrrp timers advertise** command.
Preemption is	Preemption is either enabled or disabled.
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, in seconds, of the master virtual router.
Master Down interval is	Calculated time, in seconds, that the master virtual router can be down before the backup virtual router takes over.
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).
Authentication MD5, key-string	The currently configured authentication mechanism for this group. Values for this field include “MD5” for Message Digest 5 encryption, as shown in the second example, “text, string ‘my_secret_password’” for plain text, and “key-chain ‘the_chain_i’m_looking_at’.”

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  Master   10.0.0.4        10.0.0.10
Ethernet1/0     2   105    3589          P  Master   10.0.0.4        10.0.0.20
```

Table 96 describes the fields shown in the display.

Table 96 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.
Time	Calculated time that the master virtual router can be down before the backup virtual router takes over.
Own	IP address owner.
Pre	Preemption status. 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.

Related Commands

Command	Description
vrrp ip	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

type	Interface type.
number	Interface number.
brief	(Optional) Provides a summary view of the group information.

Command Modes

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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T	This command was modified. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured.

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 enabled, delay min 4 secs
Priority is 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 enabled, delay min 2 sec
Priority is 95
Authentication MD5, key-string
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 97 describes the significant fields shown in the display.

Table 97 show vrrp interface Field Descriptions

Field	Description
Ethernet1/0 - Group 1	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 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 **vrrp timers advertise** command.
Preemption	Preemption is either enabled or disabled.
delay min	If preemption is enabled, delay min is the minimum time (in seconds) that a router will wait before preempting the current master router. This field is displayed only if the delay is set at greater than 0 seconds.
Authentication MD5, key-string	The currently configured authentication mechanism for this group. Possible values for this field include “MD5” for Message Digest 5 encryption, as shown in the example above. Other messages not displayed in the example include “text, string “‘my_secret_password’” for plain text and “key-chain ‘the_chain_i’m_looking_at’.”
Priority is 100	Priority of this group on this interface.
Master Router is 10.2.0.1 (local)	IP address of the current master virtual router.
Priority is 100	Priority of the current master router.
Master Advertisement interval	Advertisement interval of the master virtual router.
Master Down interval	Calculated time that the master virtual router can be down before the backup virtual router takes over.

Related Commands

Command	Description
vrrp ip	Enables VRRP and identifies the IP address of the virtual router.
vrrp timers advertise	Configures the interval between successive advertisements by the master virtual router in a VRRP group.

Related Commands

show vrrs clients

To display a list of Virtual Router Redundancy Service (VRRS) clients, use the **show vrrs clients** command in user EXEC or privileged EXEC mode.

show vrrs clients

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **show vrrs clients** command to display a list of VRRS clients currently active on the router. The display contains the client IDs, client priority, whether the client is interested in all VRRS groups, and the client name.

The client ID is a dynamic integer value assigned to the client when it registers with VRRS. If the client ID for a particular client is different between two versions of a Cisco IOS XE image, it means there is a change in initialization order in the two images.

The client priority is a priority that the client chooses during registration with VRRS. The client priority dictates the order in which clients receive server notifications.

Examples

The following example displays a list VRRS clients:

```
Router# show vrrs clients

ID  Priority  All-groups  Name
------------------------------
1   High      No          VRRS-Plugins
2   Low       Yes         VRRS-Accounting
3   Normal    No          PPPOE-VRRS-CLIENT
```

Table 98 describes the significant fields shown in the display.

Table 98 show vrrs clients Field Descriptions

Field	Description
Priority	Priority of the client.
All-groups	Indicates whether a client is registered for all current and future VRRS groups.
Name	Name of the client.

Related Commands

Command	Description
show vrrp	Displays a brief or detailed status of one or all configured VRRP groups on the router.
show vrrs group	Display information about VRRS groups.
show vrrs plugin database	Displays details about the internal VRRS plug-in database.
show vrrs summary	Displays a summary of all VRRS groups.

show vrrs group

To display information about Virtual Router Redundancy Service (VRRS) groups, use the **show vrrs group** command in user EXEC or privileged EXEC mode.

show vrrs group [*group-name*]

Syntax Description

group-name	Name of a VRRS group.

Command Default

Information about all VRRS groups is displayed.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **show vrrs group** command to display details of a VRRS redundancy group, if a group name is specified. If no group name is specified, details of all VRRS groups configured or added by clients on the router are displayed.

Examples

The following example displays information about all currently configured VRRS groups:

```
Router# show vrrs group

DT-CLUSTER-3
Server Not configured, state INIT, old state INIT, reason Protocol
  Address family IPv4, Virtual address 0.0.0.0, Virtual mac 0000.0000.0000
  Active interface address 0.0.0.0, standby interface address 0.0.0.0
Client 5 VRRS TEST CLIENT, priority Low

DT-CLUSTER-2
Server VRRP, state BACKUP, old state INIT, reason HA SSO
  Address family IPv4, Virtual address 10.1.1.1, Virtual mac 0000.5e00.0102
  Active interface address 10.1.1.3, standby interface address 10.1.1.2
Client 1 VRRS-Plugins, priority High
Client 2 VRRS-Accounting, priority Low
Client 3 PPPOE-VRRS-CLIENT, priority Normal

DT-CLUSTER-1
Server VRRP, state ACTIVE, old state INIT, reason HA SSO
  Address family IPv4, Virtual address 10.1.1.1, Virtual mac 0000.5e00.0101
  Active interface address 10.1.1.2, standby interface address 10.0.0.0
Client 1 VRRS-Plugins, priority High
Client 2 VRRS-Accounting, priority Low
Client 3 PPPOE-VRRS-CLIENT, priority Normal
```

Table 99 describes the significant fields shown in the display.

Table 99 show vrrs group Field Descriptions

Field	Description
state	Current state of the server.
old state	Previous state of the server
reason	Reason for the last server state change.
Address family IPv4	Address family for this VRRS group.
Virtual address 0.0.0.0	Virtual IP address for this VRRS group.
Virtual mac 0000.0000.0000	Virtual MAC address for this VRRS group.
Client 1	Client ID of a VRRS client.
VRRS-Plugins	Client name.
priority High	Priority of this client.

Related Commands

Command	Description
show vrrp	Displays a brief or detailed status of one or all configured VRRP groups on the router.
show vrrs clients	Displays a list of VRRS clients.
show vrrs plugin database	Displays details about the internal VRRS plug-in database.
show vrrs summary	Displays a summary of all VRRS groups.

show vrrs plugin database

To display details about the internal Virtual Router Redundancy Service (VRRS) plug-in database, use the **show vrrs plugin database** command in user EXEC or privileged EXEC mode.

show vrrs plugin database

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **show vrrs plugin database** command to display details of the internal VRRS plug-in database. This command maps an interface-specific configuration with a VRRS redundancy group.

The output display includes; name, server connection status, VRRS State (simple), MAC address, test control indicator, VRRS client handle, and the plug-in interface list.

Examples

The following example displays information about the internal VRRS plug-in database:

```
Router# show vrrs plugin database

VRRS Plugin Database
---------------------------------------------
Name = VRRS_NAME_1
Server connection = Live
State = Disabled
MAC addr = 0000.5e00.0101
Test Control = False
Client Handle = 3741319170
Interface list =
                 gige0/0/0.2
                 gige0/0/0.3
---------------------------------------------
Name = VRRS_NAME_2
Server connection = Diconnected
State = Disabled
MAC addr = 0000.0000.0000
Test Control = False
Client Handle = 603979779
Interface list =
                 gige0/0/0.4
---------------------------------------------
```

Related Commands

Command	Description
show vrrp	Displays a brief or detailed status of one or all configured VRRP groups on the router.
show vrrs clients	Displays a list of VRRS clients.
show vrrs group	Display information about VRRS groups.
show vrrs summary	Displays a summary of all VRRS groups.

show vrrs summary

To display a summary of all Virtual Router Redundancy Service (VRRS) groups, use the **show vrrs summary** command in user EXEC or privileged EXEC configuration mode.

show vrrs summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **show vrrs summary** command to display a summary of VRRS groups either configured on a router or added by a client. The display includes the following group information: name, server, state, and virtual address.

Examples

The following example displays a summary of VRRS groups:

```
Router# show vrrs summary

Group                                                Server State Virtual-address
------------------------------------------------------------------------------
DT-CLUSTER-3                                         UNKNOW INIT   0.0.0.0
DT-CLUSTER-2                                         VRRP   BACKUP 10.1.1.1
DT-CLUSTER-1                                         VRRP   ACTIVE 10.1.1.2
```

Table 100 describes the significant fields shown in the display.

Table 100 show vrrs summary Field Descriptions

Field	Description
Group	VRRS group name.
Server	The server which serves the VRRS group.
State	State of the server for the VRRS group.
Virtual-address	Virtual address associated with the VRRS group.

Related Commands

Command	Description
show vrrp	Displays a brief or detailed status of one or all configured VRRP groups on the router.
show vrrs clients	Displays a list of VRRS clients.
show vrrs group	Display information about VRRS groups.
show vrrs plugin database	Displays details about the internal VRRS plug-in database.

snmp-server enable traps slb

To enable IOS SLB traps for real- and virtual-server state changes, use the **snmp-server enable traps slb** command in global configuration mode. To disable the traps use the **no** form of this command.

snmp-server enable traps slb {**real** | **virtual**}

no snmp-server enable traps slb {**real** | **virtual**}

Syntax Description

real	Enables traps for real server state changes.
virtual	Enables traps for virtual server state changes.

Defaults

IOS SLB traps for real- and virtual-server state changes are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example enables IOS SLB traps for real server state changes:

```
Router(config)# snmp-server enable traps slb real
```

special-vj

To enable the special Van Jacobson (VJ) format of TCP header compression so that context IDs are included in compressed packets, use the **special-vj** command in IPHC profile configuration mode. To disable the special VJ format and return to the default VJ format, use the **no** form of this command.

special-vj

no special-vj

Syntax Description

This command has no arguments or keywords.

Command Default

Context IDs are not included in compressed packets.

Command Modes

IPHC profile configuration (config-iphcp)

Command History

Release	Modification
12.4(15)T12	This command was introduced.
15.0(1)M2	This command was integrated into Cisco IOS Release 15.0(1)M2.

Usage Guidelines

If the **special-vj** command is configured on a VJ profile, each compressed packet will include the context ID.

To enable the special VJ format of TCP header compression, use the **ip header-compression special-vj** command in interface configuration mode.

Examples

The following example shows how to enable the special VJ format of TCP header compression:

```
Router(config)# iphc-profile p1 van-jacobson
Router(config-iphcp)# special-vj
Router(config-iphcp)# end
```

Related Commands

Command	Description
ip header-compression special-vj	Enables the special VJ format of TCP header compression.
show ip tcp header-compression	Displays TCP/IP header compression statistics.

standby arp gratuitous

To configure the number of gratuitous Address Resolution Protocol (ARP) packets sent by a Hot Standby Router Protocol (HSRP) group when it transitions to the active state, and how often the ARP packets are sent, use the **standby arp gratuitous** command in interface configuration mode. To configure HSRP to send the default number of gratuitous of ARP packets at the default interval when an HSRP group changes to the active state, use the **no** form of this command.

standby arp gratuitous [**count** *number*] [**interval** *seconds*]

no standby arp gratuitous

Syntax Description

count *number*	(Optional) Specifies the number of gratuitous ARP packets to send after an HSRP group is activated. The range is 0 to 60. The default is 2. 0 sends continuous gratuitous ARP packets.
interval *seconds*	(Optional) Specifies the interval, in seconds, at which HSRP gratuitous ARP packets are sent. The range is 3 to 1800 seconds. The default is 3 seconds.

Command Default

HSRP sends one gratuitous ARP packet when a group becomes active, and then another two and four seconds later.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

You can configure HSRP to send a gratuitous ARP packet from one or more HSRP active groups. By default, HSRP sends one gratuitous ARP packet when a group becomes active, and then another two and four seconds later.

Use the **standby arp gratuitous** command in interface configuration mode to configure the number of gratuitous ARP packets sent by an Active HSRP group, and how often they are sent. The **count** and **interval** keywords can be specified in any order. If both the **count** and **interval** keywords are set to their default values, the **standby arp gratuitous** command does not appear in the running configuration.

Use the **standby send arp** command in EXEC mode to configure HSRP to send a single gratuitous ARP packet when an HSRP group becomes active.

Examples

The following example shows how to configure HSRP to send three gratuitous ARP packets every 4 seconds:

```
Router(config-if)# standby arp gratuitous count 3 interval 4
```

Related Commands

Command	Description
debug standby events	Displays events related to HSRP.
show standby arp gratuitous	Displays the number of gratuitous ARP packets sent by HSRP and how often they are sent.
standby send arp	Configures HSRP to send a single gratuitous ARP packet for each active HSRP group.

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

group-number	(Optional) Group number on the interface to which this authentication string applies. The default group number is 0.
text *string*	Authentication string. It can be up to eight characters long. The default string is cisco.
md5	Message Digest 5 (MD5) authentication.
key-string *key*	Specifies the secret key for MD5 authentication. The key can contain up to 64 characters. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the text also is unencrypted.
7	(Optional) Encrypted key.
timeout *seconds*	(Optional) Duration in seconds that HSRP will accept message digests based on both the old and new keys.
key-chain *name-of-chain*	Identifies a group of authentication keys.

Command Default

No text authentication string is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.1	The **text** keyword was added.
12.3(2)T	The **md5** keyword and associated parameters were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
service password-encryption	Encrypts passwords.
standby timers	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.

standby bfd

To reenable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering if it has been disabled on an interface, use the **standby bfd** command in interface configuration mode. To disable HSRP support for BFD, use the **no** form of this command.

standby bfd

no standby bfd

Syntax Description

This command has no arguments or keywords.

Command Default

HSRP support for BFD is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

HSRP BFD peering is enabled by default when the router is configured for BFD. Use this command to reenable HSRP BFD peering on the specified interface when it has previously been manually disabled.

To enable HSRP BFD peering globally on the router, use the **standby bfd all-interfaces** command in global configuration mode.

Examples

The following example shows how to reenable HSRP BFD peering if it has been disabled:

```
Router(config)# interface ethernet0/0
Router(config-if)# standby bfd
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
debug standby events neighbor	Displays HSRP neighbor events.
show bfd neighbor	Displays a line-by-line listing of existing BFD adjacencies.
show standby	Displays HSRP information.
show standby neighbors	Displays information about HSRP neighbors.
standby bfd all-interfaces	Reenables HSRP BFD peering on all interfaces if it has been disabled.
standby ip	Activates HSRP.

standby bfd all-interfaces

To reenable Hot Standby Router Protocol (HSRP) Bidirectional Forwarding Detection (BFD) peering on all interfaces if it has been disabled, use the **standby bfd all-interfaces** command in global configuration mode. To disable HSRP support for BFD peering, use the **no** form of this command.

standby bfd all-interfaces

no standby bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

HSRP BFD peering is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The HSRP BFD peering feature introduces BFD in the HSRP group member health monitoring system. Previously, group member monitoring relied exclusively on HSRP multicast messages, which are relatively large and consume CPU memory to produce and check. In architectures where a single interface hosts a large number of groups, there is a need for a protocol with low CPU memory consumption and processing overhead. BFD addresses this issue and offers subsecond health monitoring (failure detection in milliseconds) with a relatively low CPU impact. This command is enabled by default.

To enable HSRP support for BFD on a per-interface basis, use the **standby bfd** command in interface configuration mode.

Examples

The following example shows how to reenable HSRP BFD peering if it has been disabled on a router:

```
Router(config)# standby bfd all-interfaces
```

Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
debug standby events neighbor	Displays HSRP neighbor events.
show bfd neighbor	Displays a line-by-line listing of existing BFD adjacencies.
show standby	Displays information about HSRP.

Command	Description
show standby neighbors	Displays information about HSRP neighbors.
standby bfd	Reenables HSRP BFD peering for a specified interface if it has been disabled.
standby ip	Activates HSRP.

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-seconds* **reload** *reload-seconds*

no standby delay minimum *min-seconds* **reload** *reload-seconds*

Syntax Description

min-seconds	Minimum time (in seconds) to delay HSRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events. The valid range is 0 to 300 seconds. The default is 1 second. The recommended value is 30 seconds.
reload-seconds	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. The valid rang is 0 to 300 seconds. The default is 5 seconds. The recommended value is 60 seconds.

Command Default

HSRP group initialization is not delayed.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2	This command was introduced.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

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 all HSRP routers have the **standby delay minimum reload** configured with a minimum delay time of 30 seconds and a minimum reload time of 60 seconds.

The delay will be cancelled if an HSRP packet is received on an interface.

The **standby delay minimum reload** interface configuration command delays HSRP groups from initializing for the specified time after the interface comes up.

This command is separate from the **standby preempt delay** interface configuration command, which enables HSRP preemption delay.

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 60
 standby 3 ip 10.20.0.21
 standby 3 timers msec 300 msec 700
 standby 3 priority 100
```

Related Commands

Command	Description
show standby delay	Displays HSRP information about delay periods.
standby preempt	Configures the HSRP preemption and preemption delay.
standby timers	Configures the time between hello packets and the time before other routers declare the active HSRP or standby router to be down.

standby follow

To configure a Hot Standby Router Protocol (HSRP) group to become an IP redundancy client of another HSRP group, use the **standby follow** command in interface configuration mode. To remove the configuration of an HSRP group as a client group, use the **no** form of this command.

standby *group-number* **follow** *group-name*

no standby *group-number* **follow** *group-name*

Syntax Description

group-number	Group number on the interface for which HSRP is being activated. The default is 0.
group-name	Specifies the name of the master group for the client group to follow.

Command Default

HSRP groups are not configured as client groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **standby follow** command configures an HSRP group to become an IP redundancy client of another HSRP group.

Client or slave groups must be on the same physical interface as the master group.

A client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.

Router(config-if)# standby 1 timers 5 15
% Warning: This setting has no effect while following another group.

Router(config-if)# standby 1 preempt delay minimum 300
    % Warning: This setting has no effect while following another group.
```

HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.

You cannot configure an HSRP group to follow another HSRP group if that group is itself being followed by another HSRP group.

Use the **show standby** command to display complete information about an HSRP client group.

Examples

The following example shows how to configure HSRP group 2 as a client to the HSRP1 master group:

```
standby 2 follow HSRP1
```

Related Commands

Command	Description
show standby	Displays HSRP information.

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

group-number	(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.
ip-address	(Optional) IP address of the Hot Standby router interface.
secondary	(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 (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	The *group-number* argument was added.
11.1	The **secondary** keyword was added.
12.3(4)T	The group number range was expanded for HSRP version 2.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **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 Media Access Control (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 (000.0C07.AC*xy*), use the **no** form of this command.

standby [*group-number*] **mac-address** *mac-address*

no standby [*group-number*] **mac-address**

Syntax Description

group-number	(Optional) Group number on the interface for which HSRP is being activated. The default is 0.
mac-address	MAC address.

Command Default

If this command is not configured, and the **standby use-bia** command is not configured, the standard virtual MAC address is used: 0000.0C07.AC*xy*, 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 (config-if)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 (APN), use the MAC address to identify the first hop for outing 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 101.

Table 101 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:

```
Router(config-if)# standby 1 mac-address 4000.1000.1060
```

Related Commands

Command	Description
show standby	Displays HSRP information.
standby use-bia	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 Media Access Control (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

Syntax Description

seconds	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.

Defaults

seconds: 10 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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).

Examples

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

group-name	Specifies the name of the standby group.

Defaults

The Hot Standby Router Protocol (HSRP) is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The name specifies the HSRP group used. The HSRP group name must be unique on the router.

Examples

The following example specifies the standby name as SanJoseHA:

```
interface ethernet0
 ip address 10.0.0.1 255.0.0.0
 standby ip 10.0.0.10
 standby name SanJoseHA
 standby preempt delay sync 100
 standby priority 110
```

Related Commands

Command	Description
ip mobile home-agent redundancy	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** *seconds* | **reload** *seconds* | **sync** *seconds*}]

no standby [*group-number*] **preempt** [**delay** {**minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]

Syntax Description

group-number	(Optional) Group number on the interface to which the other arguments in this command apply.
delay	(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
minimum *seconds*	(Optional) Specifies the minimum delay period in seconds. The *seconds* argument causes the local router to postpone taking over the active role for a minimum number of seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
reload *seconds*	(Optional) Specifies the preemption delay, in seconds, after a reload only. This delay period applies only to the first interface-up event after the router has reloaded.
sync *seconds*	(Optional) Specifies the maximum synchronization period for IP redundancy clients in 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 (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(2)T	The **minimum** and **sync** keywords were added.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.2	The **reload** keyword was added.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines

Note Cisco IOS 12.2SX software releases earlier than Cisco IOS Release 12.2(33)SXH use the syntax from Cisco IOS Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Cisco IOS Release 12.2(33)SXH and later releases use Cisco IOS Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands.

When the **standby preempt** 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).

This command is separate from the **standby delay minimum reload** interface configuration command, which delays HSRP groups from initializing for the specified time after the interface comes up.

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** *seconds* 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** *seconds* 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** *seconds* command will disable the minimum delay but leave any synchronization delay if it was configured.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

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

group-number	(Optional) Group number on the interface to which the other arguments in this command apply. The default group number is 0.
priority	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 (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	The behavior of the command changed such that **standby preempt** and **standby priority** must be entered as separate commands.

Usage Guidelines



Note Cisco IOS 12.2SX software releases earlier than Cisco IOS Release 12.2(33)SXH use the syntax from Cisco IOS Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Cisco IOS Release 12.2(33)SXH and later releases use Cisco IOS Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands.

When group number 0 is used, the number 0 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 **standby track** command and another interface on the router or a tracked object goes down.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
```

Examples

In the following example, the router has a priority of 120 (higher than the default value):

```
interface ethernet 0
 standby ip 172.19.108.254
 standby priority 120
 standby preempt delay 300
```

Related Commands

Command	Description
standby track	Configures an interface so that the Hot Standby priority changes based on the availability of other interfaces.

standby redirect

To enable Hot Standby Router Protocol (HSRP) filtering of Internet Control Message Protocol (ICMP) redirect messages, use the **standby redirect** command in interface configuration mode. To disable the HSRP filtering of ICMP redirect messages, use the **no** form of this command.

standby redirect [**timers** *advertisement holddown*] [**unknown**]

no standby redirect [**unknown**]

Syntax Description

timers	(Optional) Adjusts HSRP router advertisement timers.
advertisement	(Optional) HSRP Router advertisement interval in seconds. This is an integer from 10 to 180. The default is 60 seconds.
holddown	(Optional) HSRP router holddown interval in seconds. This is an integer from 61 to 3600. The default is 180 seconds.
unknown	(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 **no standby redirect unknown** command stops the redirects from being sent.

Command Default

HSRP filtering of ICMP redirect messages is enabled if HSRP is configured on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2	The following keywords and arguments were added to the command: • **timers** *advertisement holdtime* • **unknown**
12.3(2)T	The **enable** and **disable** keywords were deprecated.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **standby redirect** 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.

With the **standby redirect** 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 redirect 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:

```
interface ethernet 0
 ip address 10.0.0.1 255.0.0.0
 standby redirect
 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:

```
interface ethernet 0
 ip address 10.0.0.1 255.0.0.0
 standby redirect timers 90 270
 standby 1 ip 10.0.0.11
```

Related Commands

Command	Description
show standby	Displays the HSRP information.
show standby redirect	Displays ICMP redirect information on interfaces configured with the HSRP.

standby redirects (global)

To configure Internet Control Message Protocol (ICMP) redirect messages with a Hot Standby Router Protocol (HSRP) virtual IP address as the gateway IP address, use the **standby redirects** command in global configuration mode. To disable the configuration, use the **no** form of this command.

standby redirects [**disable** | **enable**]

no standby redirects

Syntax Description

disable	(Optional) Disables the gateway address configuration.
enable	(Optional) Enables the gateway address configuration.

Command Default

The HSRP virtual IP address is configured as the gateway IP address.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to disable the gateway address configuration:

```
Router# configure terminal
Router(config)# standby redirects disable
```

Related Commands

Command	Description
show standby redirect	Displays ICMP redirect information on interfaces configured with the HSRP.

standby send arp

To configure Hot Standby Router Protocol (HSRP) to send a single gratuitous ARP packet for each active HSRP group, use the **standby send arp** command in user EXEC or privileged EXEC mode.

standby send arp [*interface-type interface-number* [*group-number*]]

Syntax Description

interface-type interface-number	(Optional) Interface type and number of the interface out of which ARP packets are sent.
group-number	(Optional) Group number on the interface to which the other arguments in this command apply.

Command Default

HSRP sends gratuitous ARP packets from an HSRP group when it changes to the Active state.

Command Modes

User EXEC
Privileged EXEC(#)

Command History

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

Usage Guidelines

Use the **standby send arp** command to cause a single gratuitous ARP packet to be sent for each active group. HSRP checks that the virtual IP address is entered correctly in the ARP cache prior to sending a gratuitous ARP packet. If the ARP entry is incorrect then HSRP will try to re-add it. This enables you to ensure that a host ARP cache is updated prior to starting heavy CPU-usage processes or configurations.

Static or alias ARP entries cannot be overwritten by HSRP.

You can use the **standby arp gratuitous** command in interface configuration mode to configure the number of gratuitous ARP packets sent by an active HSRP group, and how often they are sent.

Examples

The following example shows how to configure HSRP to check that an ARP cache is refreshed prior to sending a gratuitous ARP packet:

```
Router# standby send arp ethernet0/0 1
```

Related Commands

Command	Description
debug standby events	Displays events related to HSRP.
show standby arp gratuitous	Displays the number of gratuitous ARP packets sent by HSRP and how often they are sent.
standby arp gratuitous	Configures the number of gratuitous ARP packets sent by an active HSRP group, and how often they are sent.

standby sso

To enable the Hot Standby Router Protocol (HSRP) Stateful Switchover (SSO), use the **standby sso** command in global configuration mode. To disable HSRP SSO, use the **no** form of this command.

standby sso

no standby sso

Syntax Description

This command has no arguments or keywords.

Command Default

HSRP SSO is enabled when redundancy mode SSO is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **standby sso** command to enable HSRP SSO. This is the default when redundancy mode SSO is configured. When standby SSO is enabled, traffic sent using an HSRP virtual IP address continues through the HSRP group member using the current path while a Route Processor (RP) switchover occurs. The HSRP state is maintained and kept synchronized across the redundant RPs within the chassis.

If you want the traffic to switch to a redundant device (another chassis) even though the redundant RP is capable of taking over, then the feature can be disabled by using the **no** form of the command. If the command is disabled and if the primary HSRP router fails, the HSRP state is not maintained across RP switchover and traffic targeted to the HSRP virtual IP address is handled by the standby HSRP router.

Examples

The following example shows how to reenable standby SSO for HSRP if it has been disabled:

```
standby sso
```

Related Commands

Command	Description
debug standby events	Displays standby events related to HSRP.
show standby	Displays HSRP information.

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

group-number	(Optional) Group number on the interface to which the timers apply. The default is 0.
msec	(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.
hellotime	Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the **msec** option is specified, hello interval is in milliseconds. This is an integer from 15 to 999.
holdtime	Time (in seconds) before the active or standby router is declared to be down. This is an integer from *x* to 255. The default is 10 seconds. If the **msec** option is specified, *holdtime* is in milliseconds. This is an integer from *y* to 3000. Where: • *x* is the *hellotime* + 50 milliseconds, then rounded up to the nearest 1 second • *y* is greater than or equal to 3 times the *hellotime* and is not less than 50 milliseconds.

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 (config-if)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **msec** keyword was added.
12.2	The minimum values of *hellotime* and *holdtime* in milliseconds changed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **standby timers** 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.

When the **standby follow** command is used to configure an HSRP group to become an IP redundancy client of another HSRP group, the client group takes its state from the master group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:

```
Router(config-if)# standby 1 timers 5 15
% Warning: This setting has no effect while following another group.
```

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 XE Release 2.1 and Later Releases

standby track {*object-number* | *interface-type interface-number* [**decrement** *priority-decrement*]} [**shutdown**]

no standby track {*object-number* | *interface-type interface-number*}

Cisco IOS Release 12.2(33)SXH, 12.2(33)SRB, and Later Releases

standby track {*object-number* | *interface-type interface-number* [**decrement** *priority-decrement*]} [**shutdown**]

no standby track {*object-number* | *interface-type interface-number*}

Cisco IOS Release 12.4(9)T and Later Releases

standby track {*object-number* [*priority-decrement*] | *interface-type interface-number* [**decrement** *priority-decrement*]} [**shutdown**]

no standby track {*object-number* | *interface-type interface-number*}

Cisco IOS Release 12.2(15)T and Later Releases

standby track {*object-number* [*priority-decrement*] | *interface-type interface-number* [**decrement** *priority-decrement*]}

no standby track {*object-number* | *interface-type interface-number*}

Cisco IOS Releases 12.2(13)T, 12.2(14)SX, 12.2(17dSXB), 12.2(33)SRA, and Earlier Releases

standby track *interface-type interface-number* [*interface-priority*]

no standby track *interface-type interface-number* [*interface-priority*]

Syntax Description

object-number	Object number that represents the object to be tracked. The range is from 1 to 1000. The default is 1.
interface-type	Interface type (combined with interface number) that will be tracked.
interface-number	Interface number (combined with interface type) that will be tracked.
decrement *priority-decrement*	(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). The range is from 1 to 255. The default is 10.
shutdown	(Optional) Changes the HSRP group to the Init state on the basis of the state of a tracked object.

interface-priority	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The range is from 0 to 255. The default is 10.
group-number	(Optional) Group number to which the tracking applies.

Command Default There is no tracking.

Command Modes Interface configuration (config-if)

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(14)SX	Support for this command was introduced on the Cisco 7600 series routers running a Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS release 12.2(17d)SXB.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	The **shutdown** keyword was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines This command ties the Hot Standby priority of the router to the availability of its tracked objects. Use the **track interface** command or **track ip route** command 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-decrement* and *interface-priority* arguments specify 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-decrement* or *interface-priority* values or not.

The optional **shutdown** keyword configures the HSRP group to change to the Init state and become disabled rather than having its priority decremented when a tracked object goes down.

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.



Note Using the command syntax of **standby track** prior to Cisco IOS Release 12.2(15)T results in the same performance as using the new **standby track** command syntax.

If you configure HSRP to track an interface, and that interface is physically removed as in the case of an Online Insertion and Removal (OIR) operation, then HSRP regards the interface as always down. You cannot remove the HSRP interface-tracking configuration. To prevent this situation, use the **no standby track** command before you physically remove the interface.

If an object is already being tracked by an HSRP group, you cannot change the configuration to use the HSRP Group Shutdown feature that disables the HSRP group. You must first remove the tracking configuration using the **no standby track** command and then reconfigure it using the **standby track** command with the **shutdown** keyword.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

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

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
```

Router B Configuration

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
```

```
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 11
Router(config-if)# standby 1 track 100 decrement 10
```

The following example shows how to change the configuration of a tracked object to include the HSRP Group Shutdown feature:

```
Router(config-if)# no standby 1 track 101 decrement 10
Router(config-if)# standby 1 track 101 shutdown
```

Related Commands

Command	Description
show standby	Displays HSRP information.
show track	Displays information about objects that are tracked by the tracking process.
standby preempt	Configures HSRP preemption and preemption delay.
standby priority	Configures Hot Standby priority of potential standby routers.
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	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

Syntax Description

scope interface	(Optional) Specifies that this command is configured just for the subinterface on which it was entered, instead of the major interface.

Command Default

HSRP uses the preassigned MAC address on Ethernet and FDDI, or the functional address on Token Ring.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
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.
12.2(14)SX	Support for this command was added for the Cisco 7600 series routers loaded with a Supervisor Engine 720.
12.2(17d)SXB	Support for this command was extended into Cisco IOS Release 12.2(17d)SXBon the Cisco 7600 series routers loaded with a Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Note This command is not supported on Cisco 7600 series routers that are configured with a Policy Feature Card, version 2 (PFC2). The PFC2 supports a maximum of 16 unique HSRP-group numbers. You can use the same HSRP-group numbers in different VLANs. If you configure more than 16 HSRP groups, this restriction prevents use of the VLAN number as the HSRP-group number.

For an interface with this command configured, multiple standby groups can be configured. Hosts on the interface must have a default gateway configured. We recommend that you set the **no ip proxy-arp** command on the interface. It is desirable to configure the **standby use-bia** command on a Token Ring interface if there are devices that reject ARP replies with source hardware addresses set to a functional address.

When HSRP runs on a multiple-ring, source-routed bridging environment and the HRSP routers reside on different rings, configuring the **standby use-bia** command can prevent confusion about the routing information field.

Without the **scope interface** keywords, the **standby use-bia** command applies to all subinterfaces on the major interface. The **standby use-bia** command may not be configured both with and without the **scope interface** keywords at the same time.



Note Identically numbered HSRP groups use the same virtual MAC address, which might cause errors if you configure bridge groups.

Examples

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:

```
Router(config)# interface token4/0
Router(config-if)# 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 (config-if)

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.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

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

Command	Description
show standby	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* [*seconds*]]

Syntax Description

port-number	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.
password	(Optional) Text password used for generating the MD5 digest.
seconds	(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 (config-casa)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The 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
forwarding-agent	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.

sticky (firewall farm datagram protocol)

To assign all connections from a client to the same firewall, use the **sticky** command in firewall farm datagram protocol configuration mode. To remove the client/server coupling, use the **no** form of this command.

sticky *seconds*[**netmask** *netmask*] [**source** | **destination**]

no sticky

Syntax Description

seconds	Sticky timer duration in seconds. Valid values range from 0 to 65535.
netmask *netmask*	(Optional) Places the virtual server as part of a sticky subnet, for coupling of services.
source	(Optional) Bases sticky on source IP address.
destination	(Optional) Bases sticky on destination IP address.

Defaults

Virtual servers are not associated with any groups.

Command Modes

Firewall farm datagram protocol configuration (config-slb-fw-udp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(12c)E	The **source** and **destination** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that if a client's subsequent request for a firewall farm is made within 60 seconds of the previous request, then the same firewall is used for the connection:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol datagram
Router(config-slb-fw-udp)# sticky 60
```

Related Commands

Command	Description
protocol datagram	Enters firewall farm datagram protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb sticky	Displays information about the IOS SLB database.

sticky (firewall farm TCP protocol)

To assign all connections from a client to the same firewall, use the **sticky** command in firewall farm TCP protocol configuration mode. To remove the client/server coupling, use the **no** form of this command.

sticky *seconds* [**netmask** *netmask*] [**source** | **destination**]

no sticky

Syntax Description

seconds	Sticky timer duration in seconds. Valid values range from 0 to 65535.
netmask *netmask*	(Optional) Places the virtual server as part of a sticky subnet, for coupling of services.
source	(Optional) Bases sticky on source IP address.
destination	(Optional) Bases sticky on destination IP address.

Defaults

Virtual servers are not associated with any groups.

Command Modes

Firewall farm TCP protocol configuration (config-slb-fw-tcp)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(12c)E	The **source** and **destination** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies that if a client's subsequent request for a firewall farm is made within 60 seconds of the previous request, then the same firewall is used for the connection:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# protocol tcp
Router(config-slb-fw-tcp)# sticky 60
```

Related Commands

Command	Description
protocol tcp	Enters firewall farm TCP protocol configuration mode.
show ip slb firewallfarm	Displays information about the firewall farm configuration.
show ip slb sticky	Displays information about the IOS SLB database.

sticky (virtual server)

To assign all connections from a client to the same real server, use the **sticky** command in SLB virtual server configuration mode. To remove the client/server coupling, use the **no** form of this command.

sticky {*duration* [**group** *group-id*] [**netmask** *netmask*] | **asn msid** [**group** *group-id*] | **gtp imsi** [**group** *group-id*] | **radius calling-station-id** | **radius framed-ip** [**group** *group-id*] | **radius username** [**msid-cisco**] [**group** *group-id*]}

no sticky {*duration* [**group** *group-id*] [**netmask** *netmask*] | **asn msid** [**group** *group-id*] | **gtp imsi** [**group** *group-id*] | **radius calling-station-id** | **radius framed-ip** [**group** *group-id*] | **radius username** [**msid-cisco**] [**group** *group-id*]}

Syntax Description

duration	Sticky timer duration in seconds. Valid values range from 0 to 65535.
group *group-id*	(Optional) Places the virtual server in the specified sticky group, for coupling of services. All virtual servers that have the same sticky group ID share the sticky entry for a user. In essence, the **group** keyword and *group-id* argument tie multiple virtual servers together. Valid values range from 0 to 255.
netmask *netmask*	(Optional) Places the virtual server as part of the specified sticky subnet, for coupling of services. Client sessions whose source IP addresses fall within the *netmask* are directed to the same real server.
asn msid	Enables IOS SLB to load-balance Access Service Network (ASN) sessions to the same real server that processed all previous sessions for a given Mobile Station ID (MSID).
gtp imsi	Enables IOS SLB to load-balance general packet radio service (GPRS) Tunneling Protocol (GTP) Packet Data Protocol (PDP) context create requests to the same real server that processed all previous create requests for a given International Mobile Subscriber ID (IMSI).
radius calling-station-id	Enables IOS SLB to create the IOS SLB RADIUS calling-station-ID sticky database and direct RADIUS requests from a given calling station ID to the same service gateway.
radius framed-ip	Enables IOS Server Load Balancing (IOS SLB) to create the IOS SLB RADIUS framed-IP sticky database and direct RADIUS requests and non-RADIUS flows from a given end user to the same service gateway.
radius username	Enables IOS SLB to create the IOS SLB RADIUS username sticky database and direct RADIUS requests from a given end user to the same service gateway.
msid-cisco	(Optional) Enables IOS SLB to support Cisco PDSNs that provide MSID-based access (also known as MSID-based access, Cisco variant).

Defaults

Sticky connections are not tracked.
Virtual servers are not associated with any groups.

Command Modes SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(2)E	The **netmask** keyword and *netmask* argument were added.
12.1(11b)E	The **radius framed-ip** keywords were added.
12.1(12c)E	The **radius username** and **msid-cisco** keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)ZA5	The **radius calling-station-id** keywords were added.
12.2(18)SXE	The **gtp imsi** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	The **asn msid** keywords were added.

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.

In Virtual Private Network (VPN) server load balancing, remember the following requirements:

- For IPsec flows, you must specify a sticky connection between the User Datagram Protocol (UDP) virtual server and the Encapsulation Security Payload (ESP) virtual server.
- For PPTP flows, you must specify a sticky connection between the TCP virtual server and the Generic Routing Encapsulation (GRE) virtual server.
- You must specify a *duration* of at least 15 seconds.

In general packet radio service (GPRS) load balancing and the Home Agent Director, the **sticky** command is not supported.

In RADIUS load balancing, remember the following requirements:

- If you configure the **sticky radius framed-ip** command, you must also configure the **virtual** command with the **service radius** keywords specified.
- If you configure the **sticky radius calling-station-id** command or the **sticky radius username** command, you must also configure the **virtual** command with the **service radius** keywords specified, and you must configure the **sticky radius framed-ip** command.
- You cannot configure both the **sticky radius calling-station-id** command and the **sticky radius username** command on the same virtual server.
- If you configure the **sticky radius calling-station-id** command, you must configure all RADIUS maps to match against the RADIUS calling station ID attribute.
- If you configure the **sticky radius username** command, you must configure all RADIUS maps to match against the RADIUS username attribute.

For GTP load balancing:

- IOS SLB creates a sticky database object when it processes the first GTP PDP create request for a given IMSI. IOS SLB removes the sticky object when it receives a notification to do so from the real server, or as a result of inactivity. When the last PDP belonging to an IMSI is deleted on the GGSN, it sends a notification to IOS SLB to remove the sticky object.
- If you configure the **sticky gtp imsi** command, you must also configure the **virtual** command with the **service gtp** keywords specified.

For ASN load balancing, if you configure the **sticky asn msid** command, you must also configure the **virtual** command with the **service asn** keywords specified.

Examples

The following example specifies that if a client's subsequent request 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.

```
Router(config)# ip slb vserver VS1
Router(config-slb-vserver)# sticky 60 group 10
```

Related Commands

Command	Description
show ip slb sticky	Displays information about the IOS SLB database.
show ip slb vservers	Displays information about the virtual servers defined to IOS SLB.
virtual	Configures the virtual server attributes.

synguard (virtual server)

To limit the rate of TCP SYNchronize sequence numbers (SYNs) handled by a virtual server to prevent a SYN flood denial-of-service attack, use the **synguard** command in SLB virtual server configuration mode. To remove the threshold, use the **no** form of this command.

synguard *syn-count* [*interval*]

no synguard

Syntax Description

syn-count	Number of unacknowledged SYNs that are allowed to be outstanding to a virtual server. Valid values range from 0 (off) to 4294967295. The default is 0.
interval	(Optional) Interval, in milliseconds, for SYN threshold monitoring. Valid values range from 50 to 5000. The default is 100 milliseconds (ms).

Defaults

The default number of unacknowledged SYNs that are allowed to be outstanding to a virtual server is 0 (off).
The default interval is 100 ms.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In general packet radio service (GPRS) load balancing and the Home Agent Director, the **synguard** command has no meaning and is not supported.

Examples

The following example sets the threshold of unacknowledged SYNs to 50:

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# synguard 50
```

Related Commands

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

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*] | **down** *number* [**up** *number*]}

no threshold metric

Syntax Description

up	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.
down	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.
number	Threshold value. The range is from 0 to 255.

Command Default

No threshold is configured.

Command Modes

Tracking configuration (config-track)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
track ip route	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*] | **down** *number* [**up** *number*]}

no threshold percentage

Syntax Description

up	Specifies the up threshold.
down	Specifies the down threshold.
number	Threshold value. The range is from 0 to 100.

Command Default

No threshold percentage is configured.

Command Modes

Tracking configuration (config-track)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
threshold weight	Sets a threshold weight for a tracked object in a list of objects.
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.

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*] | **down** *number* [**up** *number*]}

no threshold weight [{**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}]

Syntax Description

up	Specifies the up threshold.
down	Specifies the down threshold.
number	Threshold value. The range is from 1 to 255.

Command Default

No threshold weight is configured.

Command Modes

Tracking configuration (config-track)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
threshold percentage	Sets a threshold percentage for a tracked object in a list of objects.
track list	Specifies a list of objects to be tracked and the thresholds to be used for comparison.

timeout (custom UDP probe)

To set a timeout for custom User Datagram Protocol (UDP) probes, use the **timeout** command in custom UDP probe configuration mode. To restore the default timeout, use the **no** form of this command.

timeout *seconds*

no timeout

Syntax Description

seconds	Time, in seconds, that IOS SLB waits for a response packet from the server after sending a custom UDP probe request packet. Valid range is 1 to 255. The default value is 30 seconds.

Defaults

The default custom UDP probe timeout is 30 seconds.

Command Modes

Custom UDP probe configuration

Command History

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

Examples

In the following example the custom UDP probe timeout is set to 20 seconds:

```
Router(config)# ip slb probe PROBE6 custom udp
Router(config-slb-probe)# timeout 20
```

Related Commands

Command	Description
ip slb probe custom udp	Configures a custom User Datagram Protocol (UDP) probe name and enters custom UDP probe configuration mode.
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

track

To configure an interface to be tracked where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the state of the interface, use the **track** 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

object-number	Object number in the range from 1 to 1000 representing the interface to be tracked.
interface *type number*	Interface type and number to be tracked.
line-protocol	Tracks whether the interface is up.
ip routing	Tracks whether IP routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.

Command Default

The state of the interfaces is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Use the **track** command in conjunction with the **glbp weighting** and **glbp weighting track** commands to configure parameters for an interface to be tracked. If a tracked interface on a GLBP router goes down, the weighting for that router is reduced. If the weighting falls below a specified minimum, the router will lose its ability to act as an active GLBP virtual forwarder.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, Fast Ethernet interface 0/0 tracks whether serial interfaces 2/0 and 3/0 are up. If either serial interface goes down, the GLBP weighting is reduced by the default value of 10. If both serial interfaces go down, the GLBP weighting will fall below the lower threshold and the router will no longer be an active forwarder. To resume its role as an active forwarder, the router must have both tracked interfaces back up, and the weighting must rise above the upper threshold.

```
Router(config)# track 1 interface serial 2/0 line-protocol
Router(config-track)# exit
Router(config)# track 2 interface serial 3/0 line-protocol
Router(config-track)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting 110 lower 95 upper 105
Router(config-if)# glbp 10 weighting track 1
Router(config-if)# glbp 10 weighting track 2
```

In the following example, Fast Ethernet interface 0/0 tracks whether serial interface 2/0 is enabled for IP routing, whether it is configured with an IP address, and whether the state of the interface is up. If serial interface 2/0 goes down, the GLBP weighting is reduced by a value of 20.

```
Router(config)# track 2 interface serial 2/0 ip routing
Router(config-track)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 weighting 110 lower 95 upper 105
Router(config-if)# glbp 10 weighting track 2 decrement 20
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

track application

To track the presence of Home Agent (HA), Gateway GPRS Support Node (GGSN), or Packet Data Serving Node (PDSN), traffic on a router and to enter tracking configuration mode, use the **track application** command in global configuration mode. To disable tracking of HA, GGSN, or PDSN traffic, use the no form of this command.

track *object-number* **application** {**home-agent** | **ggsn** | **pdsn**}

no track *object-number* **application** {**home-agent** | **ggsn** | **pdsn**}

Syntax Description

object-number	Number of the object to be tracked. The range is from 1 to 1000.
home-agent	Tracks Home Agent traffic on a router.
ggsn	Tracks GGSN traffic on a router.
pdsn	Tracks PDSN traffic on a router.

Command Default

Home Agent, GGSN, and PDSN traffic is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Use this command to monitor the presence of Home Agent, PDSN, and GGSN traffic on a router for mobile wireless applications.

When a redundant pair of Home Agents running HSRP between them loses connectivity, both HSRP nodes become active. Once the connectivity is restored between the two nodes, a graceful way is needed to restore proper HSRP states without losing Home Agent bindings. During the time of no connectivity, one of the nodes will continue to process Home Agent, GGSN, or PDSN traffic while the other will not. The node that continues to process traffic needs to remain active once connectivity is restored. To ensure that the active node remains in the active state, the priority of the HSRP group member that does not process Home Agent traffic is reduced. Reducing the priority of the node that is not processing Home Agent traffic ensures that this node will become the standby after connectivity is restored. When connectivity is restored, the normal Home Agent state synchronization will get all bindings back into the inactive node and, depending on the preempt configuration, it may switch over again. This state synchronization ensures that no Mobile IP, GGSN or PDSN bindings are lost.

Note The **home-agent**, **ggsn**, or **pdsn** keywords do not appear in the CLI if the corresponding application is not present in the Cisco IOS image.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows how to configure a router to track home agent traffic:

```
Router(config)# track 4 application home-agent
Router(config-track)#
```

Related Commands

Command	Description
ip mobile home-agent	Enables home agent service.
router mobile	Enables Mobile IP on the router.
service cdma pdsn	Enables PDSN service.
service gprs ggsn	Specifies that the router or Cisco IOS instance functions as a GGSN.

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

object-number	Object number that represents the interface to be tracked. The range is from 1 to 1000.
type number	Interface type and number to be tracked. No space is required between the values.
line-protocol	Tracks the state of the interface line protocol.
ip routing	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.

Command Default

No interface is tracked.

Command Modes

Global configuration (config)

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.
12.3(11)T	The **track interface ip routing** command was enhanced to allow the tracking of an IP address on an interface that was acquired through DHCP or PPP IPCP.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

This command reports a state value to clients. A tracked 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 in 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.

No space is required between the *type number* values.

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

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0:

```
Router(config)# track 1 interface serial1/0 ip routing
Router(config-track)#
```

Related Commands

Command	Description
show track	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

object-number	Object number that represents the object to be tracked. The range is from 1 to 1000.
ip-address	IP subnet address to the route that is being tracked.
/prefix-length	The number of bits that comprise the address prefix. A slash must precede the value.
reachability	Tracks whether the route is reachable.
metric threshold	Tracks the threshold metric. The default up threshold is 254 and the default down threshold is 255.

Command Default

The route to the subnet address is not tracked.

Command Modes

Global configuration (config)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

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.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, the tracking process is configured to track the reachability of 10.22.0.0/16:

```
Router(config)# 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:

```
Router(config)# track 1 ip route 10.22.0.0/16 metric threshold
```

Related Commands

Command	Description
show track	Displays HSRP tracking information.
threshold metric	Sets a threshold metric other than the default value.

track ip sla

To track the state of a Cisco IOS IP Service Level Agreements (SLAs) operation and to enter tracking configuration mode, use the **track ip sla** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track *object-number* **ip sla** *operation-number* [**state** | **reachability**]

no track *object-number* **ip sla** *operation-number* [**state** | **reachability**]

Syntax Description

object-number	Object number representing the object to be tracked. The range is from 1 to 1000.
operation-number	Number used for the identification of the IP SLAs operation you are tracking.
state	(Optional) Tracks the operation return code.
reachability	(Optional) Tracks whether the route is reachable.

Command Default

IP SLAs tracking is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced. This command replaces the **track rtr** command.
12.2(33)SXI1	This command was integrated into Cisco IOS Release 12.2(33)SXI1. This command replaces the **track rtr** command.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command replaces the **track rtr** command.
12.2(33)SRE	This command was integrated into Cisco IOS XE 12.2(33)SRE. This command replaces the **track rtr** command.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Every IP SLAs 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 IP SLAs operation can be tracked: state and reachability. The difference between these aspects relates to the acceptance of the OverThreshold return code. Table 102 shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 102 Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK	Up
	(all other return codes)	Down
Reachability	OK or over threshold	Up
	(all other return codes)	Down

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
Router(config)# track 1 ip sla 2 state
```

The following example shows how to configure the tracking process to track the reachability of IP SLAs operation 3:

```
Router(config)# track 2 ip sla 3 reachability
```

Related Commands

Command	Description
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

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

object-number	Object number of the object to be tracked. The range is from 1 to 1000.
boolean	State of the tracked list is based on a boolean calculation. The keywords are as follows: • **and**—Specifies that the list is "up" if all objects are up, or "down" if one or more objects are down. For example when tracking two interfaces, "up" means that both interfaces are up, and "down" means that either interface is down. • **or**—Specifies that the list is "up" if at least one objects is up. For example, when tracking two interfaces, "up" means that either interface is up, and "down" means that both interfaces are down.
threshold	State of the tracked list is based on a threshold. The keywords are as follows: • **percentage**—Specifies that the threshold is based on a percentage. • **weight**—Specifies that the threshold is based on a weight.

Command Default

The object list is not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command was implemented on the Cisco 7304 router.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

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:

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config-track)# exit
Router(config)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
Router(config)# track 100 list boolean and
Router(config-track)# object 1
Router(config-track)# 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:

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config-track)# exit
Router(config)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
Router(config)# track 101 list boolean or
Router(config-track)# object 1
Router(config-track)# 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:

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config-track)# exit
Router(config)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
Router(config)# track 102 threshold weight
Router(config-track)# object 1 weight 10
Router(config-track)# object 2 weight 10
Router(config-track)# 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
show track	Displays tracking information.
threshold weight	Specifies a threshold weight for a tracked list.
track list threshold percentage	Tracks a list of objects as to the up and down object states using a threshold percentage.
track list threshold weight	Tracks a list of objects as to the up and down object states using a threshold weight.
track object	Tracks an object for a tracked list as to the up and down object states.

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*}

Syntax Description

ip route	IP route for metric resolution for a specified track. The keywords and arguments are as follows: • **eigrp**—EIGRP routing protocol. The *resolution-value* argument has a range from 256 to 40000000. • **isis**—ISIS routing protocol. The *resolution-value* argument has a range from 1 to 1000. • **ospf**—OSPF routing protocol. The *resolution-value* argument has a range from 1 to 1562. • **static**—Static route. The *resolution-value* argument has a range from 1 to 100000.

Command Default

The track **ip route metric resolution** default values are used.

Command Modes

Global configuration (config)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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

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

track rtr

Note Effective with Cisco IOS Release 12.4(20)T, 12.2(33)SXI1, 12.2(33)SRE and Cisco IOS XE Release 2.4, the **track rtr** command is replaced by the **track ip sla** command. See the **track ip sla** command for more information.

To track the state of a Cisco IOS IP Service Level Agreements (SLAs) 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** *operation-number* {**state** | **reachability**}

no track *object-number* **rtr** *operation-number* {**state** | **reachability**}

Syntax Description

object-number	Object number representing the object to be tracked. The range is from 1 to 500.
operation-number	Number used for the identification of the IP SLAs operation you are tracking.
state	Tracks the operation return code.
reachability	Tracks whether the route is reachable.

Command Default

IP SLAs tracking is disabled.

Command Modes

Global configuration (config)

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.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(20)T	This command was replaced. This command was replaced by the **track ip sla** command.
12.2(33)SXI1	This command was replaced. This command was replaced by the **track ip sla** command.
Cisco IOS XE Release 2.4	This command was replaced. This command was replaced by the **track ip sla** command.
12.2(33)SRE	This command was replaced. This command was replaced by the **track ip sla** command.

Usage Guidelines

Every IP SLAs 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 IP SLAs operation can be tracked: state and reachability. The difference between these aspects relates to the acceptance of the OverThreshold return code. Table 102 shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 103 Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK	Up
	(all other return codes)	Down
Reachability	OK or over threshold	Up
	(all other return codes)	Down

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
track 1 rtr 2 state
```

The following example shows how to configure the tracking process to track the reachability of IP SLAs operation 3:

```
track 2 rtr 3 reachability
```

track stub-object

To create a stub object that can be tracked by Embedded Event Manager (EEM) and to enter tracking configuration mode, use the **track stub-object** command in global configuration mode. To remove the stub object, use the **no** form of this command.

track *object-number* **stub-object**

no track *object-number* **stub-object**

Syntax Description

object-number	Object number that represents the object to be tracked. The range is from 1 to 1000.

Command Default

No stub objects are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(31)SB3	This command was integrated into Cisco IOS Release 12.2(31)SB3.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was modified. The valid range for the *object-number* argument increased to 1000.

Usage Guidelines

Use the **track stub-object** command to create a stub object, which is an object that can be tracked and manipulated by an external process, EEM. After the stub object is created, the **default-state** command can be used to set the default state of the stub object.

EEM is a distributed, scalable, and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

As of Cisco IOS Release 15.1(3)T, a maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a router is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows how to create and configure stub object 1 with a default state of up:

```
Router(config)# track 1 stub-object
Router(config-track)# default-state up
```

Related Commands

Command	Description
default-state	Sets the default state for a stub object.
show track	Displays tracking information.

track timer

To specify the interval during which the tracking process polls the tracked object, use the **track timer** command in global configuration mode. To disable this functionality, use the **no** form of this command.

track timer {**interface** | **ip route** | **sla** } | **list** | **stub**}{ *seconds* | **msec** *milliseconds*}

no track timer {**interface** | **ip route** | **sla** } | **list** | **stub**}{ *seconds* | **msec** *milliseconds*}

Syntax Description

application	Tracks the mobile IP application polling timer.
interface	Tracks the specified interface.
ip	Tracks the specified IP protocol.
route	Tracks the IP route polling timer.
sla	Tracks the IP service level agreement (SLA) polling timer.
list	Tracks the boolean list polling timer.
stub	Tracks the Embedded Event Manager (EEM) stub polling timer.
seconds	Interval (in seconds) during which the tracking process polls the object. The range is from 1 to 3000. The default interval for interface polling is 1 second, and the default interval for IP-route polling is 15 seconds.
msec	Specifies the polling interval, in milliseconds.
milliseconds	The tracking process polling frequency interval (in milliseconds). The valid range is from 500 to 5000. All polling frequencies can be configured down to 500 milliseconds, overriding the minimum 1 second interval configured previously.

Command Default

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

Global configuration (config)

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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The **list** and **sla** keywords was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Release	Modification
15.0(1)M	This command was modified. The **application**, **msec** keywords and *milliseconds* argument was added.
12.2(33)SXI4	This command was modified. The **application**, **msec** keywords and *milliseconds* argument was added.

Examples

In the following example, the tracking process is configured to poll the tracked interface every 3 seconds:

```
Router# configure terminal
Router(config)# track timer interface 3
```

url (WSP probe)

To specify the URL path that a Wireless Session Protocol (WSP) probe is to request from the server, use the **url** command in WSP probe configuration mode. To restore the default settings, use the **no** form of this command.

url [*path*]

no url [*path*]

Syntax Description

path	(Optional) Path from the server. This argument is case-sensitive.

Defaults

If no URL path is specified, the default is /.

Command Modes

WSP probe configuration (config-slb-probe)

Command History

Release	Modification
12.1(5a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example configures a ping probe named PROBE3, enters WSP probe configuration mode, and configures the probe to request URL path http://localhost/test.txt:

```
Router(config)# ip slb probe PROBE3 wsp
Router(config-slb-probe)# url http://localhost/test.txt
```

Related Commands

Command	Description
ip slb probe wsp	Configures a Wireless Session Protocol (WSP) probe name and enters WSP probe configuration mode.
show ip slb probe	Displays information about an IOS Server Load Balancing (IOS SLB) probe.

username (IOS SLB)

To configure an ASCII regular expression string to be matched against the username attribute for RADIUS load balancing, use the **username (IOS SLB)** command in SLB RADIUS map configuration mode. To delete the username match string, use the **no** form of this command.

username *string*

no username *string*

Syntax Description

string	ASCII regular expression string to be matched against the username attribute in the RADIUS payload. For information about regular expressions and how to use them in Cisco IOS software configurations, refer to the "Understanding Regular Expressions" section of the "Using the Cisco IOS Command-Line Interface" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*: http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

Defaults

None

Command Modes

SLB RADIUS map configuration (config-slb-radius-map)

Command History

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

Usage Guidelines

For a given IOS SLB RADIUS map, you can configure a single **calling-station-id** command or a single **username (IOS SLB)** command, but not both.

Examples

The following example specifies that, for IOS SLB RADIUS map **1**, string **...?525*** is to be matched against the username attribute in the RADIUS payload:

```
Router(config)# ip slb map 1 radius
Router(config-slb-radius-map)# username ...?525*
```

Related Commands

Command	Description
calling-station-id	Configures an ASCII regular expression string to be matched against the calling station ID attribute in the RADIUS payload.
ip slb map	Configures an IOS SLB protocol map and enters SLB map configuration mode.

Command	Description
show ip slb map	Displays information about IOS SLB protocol maps.

virtual

To configure virtual server attributes, use the **virtual** command in SLB virtual server configuration mode. To remove the attributes, use the **no** form of this command.

Encapsulation Security Payload (ESP) and Generic Routing Encapsulation (GRE) Protocols

virtual *ipv4-address* [*ipv4-netmask* [**group**]] {**esp** | **gre** | *protocol*}

no virtual *ipv4-address* [*ipv4-netmask* [**group**]] {**esp** | **gre** | *protocol*}

TCP and User Datagram Protocol (UDP)

virtual *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]

no virtual *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]

Syntax Description

ipv4-address	IPv4 address for this virtual server instance, used by clients to connect to the IPv4 real servers through the IPv4 server farm.
ipv4-netmask	(Optional) IPv4 network mask for transparent web cache load balancing. The default is 0.0.0.0 (all subnets).
group	(Optional) Allows the virtual subnet to be advertised. If you do not specify the **group** keyword, the virtual subnet cannot be advertised.
esp	Performs load balancing for only Encapsulation Security Payload (ESP) connections.
gre	Performs load balancing for only Generic Routing Encapsulation (GRE) connections.
protocol	Protocol for which load balancing is performed. The valid range is 2 to 127.
ipv6 *ipv6-address*	(Optional) For dual-stack, IPv6 address for this virtual server instance, used by IPv6 clients to connect to IPv6 real servers through the IPv6 server farm.
prefix *ipv6-prefix*	(Optional) For dual-stack, IPv6 prefix.
tcp	Performs load balancing for only TCP connections.
udp	Performs load balancing for only User Datagram Protocol (UDP) connections.
port	(Optional) IOS Server Load Balancing (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 *port* argument are as follows: • All ports: **any 0** • Access Service Network (ASN): **asn 2231** • Connectionless secure Wireless Session Protocol (WSP): **wsp-wtls 9202**

port (continued)	• Connectionless WSP: **wsp 9200** • Connection-oriented secure WSP: **wsp-wtp-wtls 9203** • Connection-oriented WSP: **wsp-wtp 9201** • Domain Name System: **dns 53** • File Transfer Protocol: **ftp 21** • General packet radio service (GPRS) tunneling protocol (GTP) v0: **gtp 3386** • GTP v1 or v2: **gtp 2123** • HTTP over Secure Socket Layer: **https 443** • Internet Key Exchange (IKE): **isakmp 500** • Mapping of airline traffic over IP, Type A: **matip-a 350** • Network News Transport Protocol: **nntp 119** • Post Office Protocol v2: **pop2 109** • Post Office Protocol v3: **pop3 110** • Simple Mail Transport Protocol: **smtp 25** • Telnet: **telnet 23** • X.25 over TCP (XOT): **xot 1998** • World Wide Web (HTTP): **www 80** Specify a port number of 0 to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports except GTP ports).
any	(Optional) Performs load balancing on all ports.
service *service*	(Optional) Couples connections associated with a given service, such as HTTP or Telnet, so all related connections from the same client use the same real server. The following are the valid types of connection coupling: • **asn**—Enables ASN load balancing. • **ftp**—Couples FTP data connections with the control session that created them. • **gtp**—Enables GPRS load balancing without general packet radio service (GPRS) tunneling protocol (GTP) cause code inspection enabled, which allows load-balancing decisions to be made using Layer 5 information. You can balance UDP flows without awareness of GTP by omitting the **service gtp** keywords. • **gtp-inspect**—Enables GPRS load balancing with GTP cause code inspection enabled. • **ipmobile**—Enables the Home Agent Director. • **per-packet**—Does not maintain connection objects for packets destined for this virtual server. • **radius**—Enables IOS SLB to build RADIUS session objects for RADIUS load balancing.

Command Default No default behavior or values.

Command Modes SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(5a)E	The **wsp**, **wsp-wtp**, **wsp-wtls**, and **wsp-wtp-wtls** keywords were added.
12.1(9)E	The **gtp** option was added as a new value on the *service* argument.
12.1(11b)E	The following keywords, arguments, and options were added: • The **esp**, **gre**, and **all** keywords • The *protocol* argument • The **isakmp** option on the *port* argument • The **per-packet** and **radius** options on the *service* argument The **wsp**, **wsp-wtp**, **wsp-wtls**, and **wsp-wtp-wtls** keywords were changed to options for the *port* argument.
12.1(12c)E	The **group** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp-inspect** option was added as a new value on the *service* argument.
12.2(14)ZA2	The **ipmobile** option was added as a new value on the *service* argument.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	The **asn** option was added on the *service* argument.
15.0(1)S	The **ipv6** *ipv6-address* and **prefix** *ipv6-prefix* options were added.

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 IOS SLB. 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 or any.

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.

Specifying port 9201 for connection-oriented WSP mode also activates the Wireless Application Protocol (WAP) finite state machine (FSM), which monitors WSP and drives the session FSM accordingly.

In RADIUS load balancing, IOS SLB maintains session objects in a database to ensure that re-sent RADIUS requests are load-balanced to the same real server.

IOS SLB supports general packet radio service (GPRS) Tunneling Protocol (GTP) v0, v1, and v2 real servers. A GTP v0 or v1 real server cannot manage GTP v2 requests. Therefore, you must configure separate virtual servers for GTPv2 real servers and for GTP v0 or v1 real servers.

IOS SLB supports dual-stack addresses for GTP load balancing only. To support dual-stack addresses:

- You must configure the virtual server as a dual-stack virtual server, with the virtual IPv4 and IPv6 addresses and the optional IPv6 prefix, using this command.
- You must associate an IPv6 server farm with the dual-stack virtual server.

Examples

The following example specifies that the virtual server with the IPv4 address 10.0.0.1 performs load balancing for TCP connections for the port named www. The virtual server processes HTTP requests.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.1 tcp www
```

The following example specifies that the virtual server with the IPv4 address 10.0.0.13 performs load balancing for UDP connections for all ports. The virtual server processes HTTP requests.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.13 udp 0
```

Related Commands

Command	Description
ip slb vserver	Identifies a virtual server.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).

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* | **text** *text-string* | **md5** {**key-chain** *key-chain* | **key-string** [**0** | **7**] *key-string* [**timeout** *seconds*]}}

no vrrp *group* **authentication** {*text-string* | **text** *text-string* | **md5** {**key-chain** *key-chain* | **key-string** [**0** | **7**] *key-string* [**timeout** *seconds*]}}

Syntax Description

group	Virtual router group number for which authentication is being configured. The group number is configured with the **vrrp ip** command. The valid range is 1 to 255.
text-string	Plain text authentication. There is no default value.
text *text-string*	Plain text authentication. The *text-string* argument is the authentication string and can be up to eight alphanumeric characters. There is no default value.
md5	Message digest 5 (MD5) authentication. The arguments and keywords are as follows: • **key-chain**—Authentication using a live key and key ID. The *key-chain* argument specifies a string and must match the assigned key-chain name using the **key chain** command. • **key-string**—Specifies the secret key for the MD5 authentication string. The arguments and keywords are as follows: – **0**—(Optional) The key is unencrypted. – **7**—(Optional) The key is encrypted. – *key-string*—Up to 64 characters. It is recommended that the string be at least 16 characters. No prefix to the *key-string* argument means that the key is unencrypted. – **timeout** *seconds* —(Optional) Duration in seconds that VRRP will accept message digests based on both the old and new keys. **Note** The key-string authentication method is encrypted if the **service password-encryption** command has been specified.

Command Default

VRRP authentication is disabled.

Command Modes

Interface configuration (config-if)

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(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(14)T	The **md5**, **key-string**, **0**, **7**, and **key-chain** keywords were added. The *text-string*, *key-string*, and *key-chain* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(31)SG	This command was integrated into Cisco IOS Release 12.2(31)SG.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

VRRP does not accept a virtual router group number 0 and never has an empty group. The valid range for the VRRP group is 1 to 255.

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. The authentication string is sent unencrypted in all VRRP messages when using the **vrrp authentication text** *text-string* option.

All routers within the VRRP group must be configured with the same authentication string. If the same authentication string is not configured, the routers in the VRRP group will not communicate with each other and any misconfigured router in the group will change its state to master.

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

Note Plain text authentication is not meant to be used for security. It simply provides a way to prevent a router that does not belong to a configured VRRP group from participating in it.

The **timeout** *seconds* keyword and argument specify the duration that the VRRP group will accept message digests based on both the old and new keys. This option allows time for configuration of all routers in a group with the new key. VRRP route flapping can be minimized by changing the keys on all the routers, provided that the master router is changed last. The master router should have its key string changed no later than one holdtime period, specified by the **vrrp timers advertise** interface configuration command, after the backup routers. This procedure ensures that the backup routers do not time out the master router.

Examples

The following example shows how to configure an authentication text string of x30dn78k:

```
vrrp 1 authentication x30dn78k
```

The following example shows how to configure an MD5 key string:

```
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
```

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
key chain	Enables authentication for routing protocols.
service password-encryption	Encrypts passwords.
vrrp ip	Enables VRRP and identifies the IP address of the virtual router.
vrrp timers advertise	Configures the interval between successive advertisements by the master virtual router in a VRRP group.

vrrp delay

To configure the delay period before the initialization of all Virtual Router Redundancy Protocol (VRRP) groups on an interface, use the **vrrp delay** command in interface configuration mode. To remove all configured delays, use the **no** form of this command.

vrrp delay {**minimum** *seconds* [**reload** *seconds*] | **reload** *seconds*}

no vrrp delay {**minimum** *seconds* [**reload** *seconds*] | **reload** *seconds*}

Syntax Description

minimum *seconds*	The minimum time, in seconds, to delay VRRP group initialization after an interface comes up. Valid range is 1–10000.
reload *reload-seconds*	Time, in seconds, to delay after the router has reloaded. Valid range is 0–10000.

Command Default

No delay value is used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **vrrp delay** command to configure the delay period before the initialization of VRRP groups. This command applies to all VRRP groups on an interface. This command cannot be configured per-VRRP group.

The **minimum** *seconds* value is the minimum time (in seconds) to delay VRRP group initialization after an interface comes up. This minimum delay period applies to all subsequent interface events.

The **reload** *seconds* value is the time period to delay after the router has reloaded. This delay period applies only to the first interface-up event after the router has reloaded.

The recommended **minimum** *seconds* value is 30 seconds and the recommended **reload** *seconds* value is 60 seconds.

The **no vrrp delay** command removes all delays, and is equivalent to configuring 0 for each argument. When the **no vrrp delay** command is configure, there is no appreciable delay between the interface coming up and the VRRP groups on that interface becoming operational.

Examples

The following example shows how to configure a minimum delay of 30 seconds and a reload delay of 60 seconds:

```
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# vrrp delay minimum 30 reload 60
```

Related Commands

Command	Description
vrrp name	Links a VRRS client to a VRRP group.

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

group	Virtual router group number. The group number range is from 1 to 255.
text	Text (up to 80 characters) that describes the purpose or use of the group.

Command Default

There is no description of the VRRP group.

Command Modes

Interface configuration (config-if)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
vrrp ip	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

group	Virtual router group number. The group number range is from 1 to 255.
ip-address	IP address of the virtual router.
secondary	(Optional) Indicates additional IP addresses supported by this group.

Command Default

VRRP is not configured on the interface.

Command Modes

Interface configuration (config-if)

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(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(31)SG	This command was integrated into Cisco IOS Release 12.2(31)SG.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **vrrp ip** command activates VRRP on the configured interface. The first IP address specified in the VRRP configuration is used as the primary address for the virtual router. For VRRP to elect a designated router, at least one router on the cable must have been configured with the primary address of the virtual router. Configuration of the primary address on the master router always overrides a primary address that is currently in use.

VRRP does not support address learning. All addresses must be configured.

All routers in the VRRP group must be configured with the same primary address for the virtual router. If different primary addresses are configured, the routers in the VRRP group will not communicate with each other and any misconfigured routers in the group will change their state to master.

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 You can configure the primary IP address of a VRRP group with the same address as the interface. When VRRP is configured in this manner, the router that has the interface IP address is always the master router. Removing the VRRP configuration from a router configured in this way and leaving the IP address of the interface active is considered a misconfiguration because duplicate IP addresses on the LAN will result. If you have configured VRRP in this way and need to remove the VRRP configuration, you can change the interface address to a different value. Alternately, you can also remove all VRRP group members that are using the virtual address equal to the interface address on the router. To avoid a period of duplicate address warnings, deconfigure all VRRP routers in the group. This leaves the address owner router the last to be deconfigured, which avoids duplicate address warnings.

VRRP must be in the master state for proxy Address Resolution Protocol (ARP) to use the VRRP virtual MAC address.

Examples

The following example shows how to enable 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
show vrrp	Displays a summary or detailed status of one or all configured VRRP groups.

vrrp name

To link a Virtual Router Redundancy Service (VRRS) client to a Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp name** command in interface configuration mode. To disassociate a VRRS group from VRRS, use the **no** form of this command.

vrrp *group-number* **name** [*vrrp-group-name*]

no vrrp *group-number* **name** [*vrrp-group-name*]

Syntax Description

group-number	Virtual router group number. The group number range is from 1 to 255.
vrrp-group-name	(Optional) VRRP group name.

Command Default

VRRS clients are not linked to VRRP groups.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **vrrp name** command to link VRRS clients to VRRP groups. VRRP provides stateless redundancy for IP routing. VRRP by itself is limited to maintaining its own state. Linking a VRRS client to a VRRP group allows client applications to implement stateful failover. IP redundancy clients are other Cisco IOS processes or applications that use VRRP to provide or withhold a service or resource dependent upon the state of the group.

Use the **no vrrp name** command to dissociates a VRRP group from VRRS. After this, the same VRRP group can be attached to a different VRRP name; or the VRRS name can be applied to a different VRRP group.

Examples

The following example shows how to link VRRS clients to a VRRP group named VRRP-Partition-1:

```
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# vrrp 1 name VRRP-Partition-1
```

Related Commands

Command	Description
vrrs follow	Configures a name association between VRRS plug-ins and the VRRS server.
vrrp name	Links a VRRS client to a VRRP group.

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 function, use the **no** form of this command.

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

no vrrp *group* **preempt**

Syntax Description

group	Virtual router group number of the group for which preemption is being configured. The group number is configured with the **vrrp ip** command. The group number range is from 1 to 255.
delay minimum *seconds*	(Optional) Number of seconds that the router will delay before issuing an advertisement claiming master ownership. The default delay is 0 seconds.

Defaults

This command is enabled.

Command Modes

Interface configuration (config-if)

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(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(31)SG	This command was integrated into Cisco IOS Release 12.2(31)SG.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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 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 minimum 15
vrrp 1 priority 200
```

Related Commands

Command	Description
vrrp ip	Enables VRRP and identifies the IP address of the virtual router.
vrrp priority	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. The group number range is from 1 to 255.
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 (config-if)

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

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
vrrp ip	Enables VRRP and identifies the IP address of the virtual router.
vrrp preempt	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 shutdown

To disable the Virtual Router Redundancy Protocol (VRRP) group on an interface, use the **vrrp shutdown** command in interface configuration mode.

vrrp *group-number* **shutdown**

Syntax Description

group-number	Virtual router group number. The group number range is from 1 to 255.

Defaults

VRRP groups configured by the **vrrp** *group-number* **ip** command are enabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(11)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

When a VRRP group has been configured using the **vrrp** *group-number* **ip** command, the protocol is fully operational. The **vrrp shutdown** command is not displayed on the router, and to disable the protocol for one group, you must explicitly specify the group using the **vrrp shutdown** command.

Examples

The following example shows how to disable one VRRP group on Ethernet interface 0/1 (group 1) while retaining the VRRP group on Ethernet interface 0/2 (group 2):

```
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
```

Related Commands

Command	Description
show vrrp	Displays a summary or detailed status of one or all configured VRRP groups.
vrrp ip	Enables the VRRP on an interface and identify the IP address of the virtual router.

vrrp sso

To enable Virtual Router Redundancy Protocol (VRRP) support of Stateful Switchover (SSO) if it has been disabled, use the **vrrp sso** command in global configuration mode. To disable VRRP support of SSO, use the **no** form of this command.

vrrp sso

no vrrp sso

Syntax Description

This command has no arguments or keywords.

Command Default

VRRP support of SSO is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to enable VRRP support of SSO if it has been manually disabled by the **no vrrp sso** command.

Examples

The following example shows how to disable VRRP support of SSO:

```
Router(config)# no vrrp sso
```

Related Commands

Command	Description
debug vrrp all	Displays debugging messages for VRRP errors, events, and state transitions.
debug vrrp ha	Displays debugging messages for VRRP high availability.
show vrrp	Displays a brief or detailed status of one or all configured VRRP groups.

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

group	Virtual router group number. The group number range is from 1 to 255.
msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.
interval	Time interval between successive advertisements by the master virtual router. The unit of the interval is in seconds, unless the **msec** keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the **msec** keyword is specified, the valid range is 50 to 999 milliseconds.

Defaults

interval: 1 second

Command Modes

Interface configuration (config-if)

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(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(31)SG	This command was integrated into Cisco IOS Release 12.2(31)SG.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

The **vrrp timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer values are not configured can learn timer values from the master router. The timers configured on

the master router always override any other timer settings. All routers in a VRRP group must use the same timer values. If the same timer values are not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.

Examples

The following example shows how to configure the master virtual router to send advertisements every 4 seconds:

```
vrrp 1 timers advertise 4
```

Related Commands

Command	Description
vrrp ip	Enables VRRP and identifies the IP address of the virtual router.
vrrp timers learn	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**

Syntax Description

group	Virtual router group number to which the command applies. The group number range is from 1 to 255.

Defaults

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 **vrrp timers advertise** command.

Command Modes

Interface configuration (config-if)

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(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(31)SG	This command was integrated into Cisco IOS Release 12.2(31)SG.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

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.

Examples

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
```

Related Commands

Command	Description
vrrp ip	Enables VRRP and identifies the IP address of the virtual router.
vrrp timers advertise	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* **track** *object-number* [**decrement** *priority*]

no vrrp *group* **track** *object-number* [**decrement** *priority*]

Syntax Description

group	Group number to which the tracking applies. The group number range is from 1 to 255.
object-number	Object number in the range from 1 to 500 representing the object to be tracked.
decrement *priority*	(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 (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can 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
track interface	Configures an interface to be tracked.
track ip route	Tracks the state of an IP route.

vrrs

To specify a distinct AAA accounting method list to use, a non-zero delay time for accounting-off messages, and additional attributes other than the default for a Virtual Router Redundancy Protocol (VRRP) group, enter the **vrrs** command in the global configuration mode. To return to the default values, use the **no** form of this command.

vrrs *vrrs-group-name*

no vrrs *name*

Syntax Description

vrrs-group-name	Name of a VRRS group.

Command Default

Accounting-on and accounting-off messages for a VRRP group are set with default accounting attributes, without any delay for accounting-off messages, and using the VRRS default accounting method list.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

The VRRS group name specified by the *vrrs-group-name* argument should match a VRRP group as configured by the **vrrp name** command in interface configuration mode.

Note VRRS does not perform a cross-check of the VRRS group name between the **vrrs** global configuration command and the **vrrp name** interface configuration command. Any string entered is accepted.

.The following RADIUS attributes are included in accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, vrrs
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Type
- Attribute 44 Acct-Session-Id

Examples

The following example shows how to configure a VRRS group named vrrp-group-1:

```
Router(config)# vrrs vrrp-group-1
```

```
Router(config-vrrs)# exit
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 1 name vrrp-group-1
```

Related Commands

Command	Description
vrrp ip	Enables the VRRP on an interface and identifies the IP address of the virtual router.
vrrp name	Links a VRRS client to a VRRP group.

vrrs follow

To configure a name association between Virtual Router Redundancy Service (VRRS) plug-ins and the VRRS server, use the **vrrs follow** command in subinterface configuration mode. To disassociate the VRRS plug-ins from a server, use the **no** form of this command.

vrrs follow *name*

no vrrs follow *name*

Syntax Description

name	A name that associates the VRRS plug-ins with a First Hop Redundancy Protocol (FHRP) server, via VRRS, that shares the same name.

Command Default

VRRS plug-ins remain detached and in the DOWN state.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

This command can be applied only to subinterfaces.

The **no vrrs follow** command disassociate the VRRS plug-ins from a server. The VRRS plug-ins are disabled after this, and are forced to the DOWN state until they are reattached to a new name.

Examples

The following example configures a name association between the VRRS interface-state and mac-address plug-ins and the VRRS server:

```
Router(config)# interface gigabitethernet0/0/0.1
Router(config-subif)# ip address 172.24.1.1 255.255.255.0
Router(config-subif)# vrrs follow name1
Router(config-subif)# vrrs interface-state
Router(config-subif)# vrrs mac-address
```

Related Commands

Command	Description
vrrs interface-state	Configures the VRRP shutdown plug-in on an interface.
vrrs mac-address	Configures the VRRS mac-address plug-in on an interface.

vrrs interface-state

To configure the Virtual Router Redundancy Protocol (VRRP) shutdown plug-in on an interface, use the **vrrs interface-state** command in subinterface configuration mode. To disable the shutdown plug-in, use the **no** form of this command.

vrrs interface-state

no vrrs interface-state

Syntax Description

This command has no arguments or keywords.

Command Default

The VRRS shutdown plug-in remains detached and in the DOWN state.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **vrrs interface-state** command to configure the VRRP shutdown plug-in on an interface. When the line protocol is configured, and the Virtual Router Redundancy Service (VRRS) is in a nonactive state, the line protocol state of the interface is transitioned to down.

The **vrrs follow** command associates the interface-state plug-in with a First Hop Redundancy Protocol (FHRP) that is using the same name with VRRS. Removal of the **vrrs interface-state** command, or a change in the VRRS state to an active state, causes the line protocol state of the interface to transition to UP.

Examples

The following example shows how to configure the VRRP shutdown plug-in on an interface:

```
Router(config)# interface gigabitethernet0/0/1.1
Router(config-subif)# ip address 10.0.0.0 255.255.255.0
Router(config-subif)# vrrs follow vrrp-partition-1
Router(config-subif)# vrrs interface-state
Router(config-subif)# vrrs mac-address arp interval 5 duration 60
```

Related Commands

Command	Description
vrrs follow	Configures a name association between VRRS plug-ins and the VRRS server.
vrrs mac-address	Configures the VRRS mac-address plug-in on an interface.

vrrs mac-address

To configure the Virtual Router Redundancy Service (VRRS) mac-address plug-in on an interface, use the **vrrs mac-address** command in subinterface configuration mode. To disable the mac-address plug-in, use the **no** form of this command.

vrrs mac-address [**arp** [**interval** *seconds*] [**duration** *seconds*]]

no vrrs mac-address [**arp** [**interval** *seconds*] [**duration** *seconds*]]

Syntax Description

arp	(Optional) Enables sending gratuitous ARP messages.
interval *seconds*	(Optional) Specifies, the interval, in seconds, at which gratuitous ARPs are sent by the VRRS mac-address plug-in.
duration *seconds*	(Optional) Specifies, in seconds, how long the gratuitous ARP repeats continue. A value of 0 means indefinitely, but use of this option should be carefully considered because it may have a detrimental effect on the performance of the router or network.

Command Default

The VRRS mac-address plug-in remains detached and in the DOWN state.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **vrrs mac-address** command to configure the VRRS mac-address plug-in on an interface. When a virtual-MAC is configured, and VRRS is in an ACTIVE state, a virtual-MAC is added to the interface that is to be associated with the Primary IP address configured on that interface. Use the **vrrs follow** command to associate the mac-address plug-in with a First Hop Redundancy Protocol (FHRP) that is using the same name as VRRS. The mac-address plug-in can be enabled with all defaults by configuring the **vrrs mac-address** command with no optional keywords or arguments.

Examples

The following example shows how to configure the VRRS mac-address plug-in on an interface:

```
Router(config)# interface gigabitethernet0/0/1.1
Router(config-subif)# ip address 10.0.0.0 255.255.255.0
Router(config-subif)# vrrs follow vrrp-partition-1
Router(config-subif)# vrrs interface-state
Router(config-subif)# vrrs mac-address arp interval 5 duration 60
```

Related Commands

Command	Description
vrrs follow	Configures a name association between VRRS plug-ins and the VRRS server.
vrrs interface-state	Configures the VRRP shutdown plug-in on an interface.

weight (firewall farm real server)

To specify a real server's capacity, relative to other real servers in the firewall farm, use the **weight** command in firewall farm real server configuration mode. To restore the default weight value, use the **no** form of this command.

weight *setting*

no weight

Syntax Description

setting	Weight setting to use for the real server predictor algorithm. Valid settings range from 1 to 255. The default weight setting is 8.

Defaults

The default setting to use for the real server predictor algorithm is 8.

Command Modes

Firewall farm real server configuration (config-slb-fw-real)

Command History

Release	Modification
12.1(3a)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies the relative weights of three real servers as 16, 8 (by default), and 24, respectively:

```
Router(config)# ip slb firewallfarm FIRE1
Router(config-slb-fw)# real 10.10.1.1
Router(config-slb-fw-real)# weight 16
Router(config-slb-fw-real)# inservice
Router(config-slb-fw-real)# exit
Router(config-slb-fw)# real 10.10.1.2
Router(config-slb-fw-real)# inservice
Router(config-slb-fw-real)# exit
Router(config-slb-fw)# real 10.10.1.3
Router(config-slb-fw-real)# weight 24
```

Related Commands

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

weight (real server)

To specify a real server's capacity, relative to other real servers in the server farm, use the **weight** command in SLB real server configuration mode. To restore the default weight value, use the **no** form of this command.

weight *setting*

no weight

Syntax Description

setting	Weight setting to use for the real server predictor algorithm. Valid settings range from 1 to 255. The default weight setting is 8.

Defaults

The default setting to use for the real server predictor algorithm is 8.

Command Modes

SLB real server configuration (config-slb-sfarm)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The static weights you define using this command are overridden by the weights calculated by Dynamic Feedback Protocol (DFP). If DFP is removed from the network, IOS Server Load Balancing (IOS SLB) reverts to these static weights.

Examples

The following example specifies the relative weights of three real servers as 16, 8 (by default), and 24, respectively:

```
Router(config)# ip slb serverfarm PUBLIC
!-----First real server
Router(config-slb-sfarm)# real 10.10.1.1
!-----Assigned weight of 16
Router(config-slb-real)# weight 16
!-----Enabled
Router(config-slb-real)# inservice
Router(config-slb-real)# exit
!-----Second real server
Router(config-slb-sfarm)# real 10.10.1.2
!-----Enabled with default weight
Router(config-slb-real)# inservice
```

```
Router(config-slb-real)# exit
!-----Third real server
Router(config-slb-sfarm)# real 10.10.1.3
!-----Assigned weight of 24, not enabled
Router(config-slb-real)# weight 24
```

Related Commands

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