Cisco IOS IP Application Services Command Reference

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

CONTENTS

Introduction

Introduction

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

- Enhanced Object Tracking (EOT)
- IP Services
- IPv4 Broadcast Packet Handling
- Stream Control Transmission Protocol (SCTP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Web Cache Control Protocol (WCCP)

Introduction

A through F

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

Syntax Description

This command has no arguments or keywords.

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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

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 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.

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.

Command	Description
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.
track ip sla	Tracks the state of a Cisco IOS SLAs operation and enters tracking configuration mode.
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 timer	Specifies the interval that a tracking process polls a tracked object.

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.

Command	Description
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-typeinterface-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 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.

Command Default

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.

Command	Description
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 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-type	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)* .
15.1(4)M	This command was modified. The optional **interface** keyword and associated *type* and *number* arguments were added. 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
```

The following example shows how to clear the IP traffic statistics on Ethernet interface 0/0:

```
Router# clear ip traffic interface ethernet 0/0
```

The following is sample output from the **show ip traffic** command for Ethernet interface 0/0 after clearing the traffic using the **clear ip traffic** command:

```
Router# show ip traffic

Ethernet0/0 IP-IF statistics :
  Rcvd:  0 total, 0 total_bytes
         0 format errors, 0 hop count exceeded
         0 bad header, 0 no route
         0 bad destination, 0 not a router
         0 no protocol, 0 truncated
         0 forwarded
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 discards, 0 delivers
  Sent:  0 total, 0 total_bytes 0 discards
         0 generated, 0 forwarded
         0 fragmented into, 0 fragments, 0 failed
  Mcast: 0 received, 0 received bytes
         0 sent, 0 sent bytes
  Bcast: 0 received, 0 sent
```

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 IPv4 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*] [*service-number*] [**web-cache**] [**default**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance to associate with a service group.
service-number	(Optional) Number of the cache service to be removed. The number can be from 0 to 254.
web-cache	(Optional) Directs the router to remove statistics for the web cache service.

Command Default

WCCP statistics are not removed.

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.

Release	Modification
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

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.

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.

Command Default

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.

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(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**] **statisticscounters**| **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.

Command	Description
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.

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.

Command Default

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.

clear wccp

To remove all (IPv4 and IPv6) Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service, use the **clear wccp** command in privileged EXEC mode.

clear wccp[**vrf***vrf-name*][*service-number*][**web-cache**][**default**]

Syntax Description

vrf *vrf-name*	(Optional) Directs the router to remove statistics for a specific virtual routing and forwarding (VRF) instance.
service-number	(Optional) Number of the cache service to be removed. The number can be from 0 to 254.
web-cache	(Optional) Directs the router to remove statistics for the web cache service.
default	(Optional) Directs the router to remove statistics for the default routing table.

Command Default

WCCP statistics are not removed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ip wccp	Enables support of the specified WCCP service for participation in a service group.
ipv6 wccp	Enables support of the specified WCCP service for participation in a service group.
show wccp	Displays global statistics related to the WCCP.

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.
12.2(50)SY	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, 15.1(1)S and 12.2(50)SY, 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.
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:

```
Router(config)# track 2 stub
Router(config-track)# default-state up
```

Related Commands

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

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

Command Default

No delay time for communicating state changes 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)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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

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 tracked object state changing to down is set to 30 seconds.

```
Router(config)# track 1 ip route 10.22.0.0/16 metric threshold
Router(config-track)# threshold metric up 16 down 20
Router(config-track)# delay down 30
```

Related Commands

Command	Description
show track	Displays HSRP tracking information.
threshold metric	Sets a threshold metric.
track ip route	Tracks the state of an IP route.

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.

Command Default

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:

```
Router(config-casa)# forwarding-agent 1637
```

Related Commands

Command	Description
show ip casa oper	Displays operational information about the Forwarding Agent.

ip accounting through ip sctp authenticate

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.

Command Default

IP accounting is disabled on an interface.

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:

```
Router(config)# interface ethernet 0
Router(config-if)# 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.

Command Default

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:

```
Router(config)# 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.

Command	Description
ip accounting	Enables IP accounting on an interface.
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 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.

Command Default

IP accounting is disabled on an interface.

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:

```
Router(config)# interface ethernet 4/0/0
Router(config-if)# ip accounting mac-address input
Router(config-if)# ip accounting mac-address output
```

Examples

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:

```
Router(config)# interface ethernet 4/0/0
Router(config-if)# ip accounting precedence input
Router(config-if)# 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.

Command Default

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:

```
Router(config)# 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.
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.

Command Default

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:

```
Router(config)# 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.

Command Default

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:

```
Router(config-if)# 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.

Command Default

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:

```
Router(config)# 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 the route processor is using NHRP in distributed Cisco Express Forwarding switching mode, this value must be set to 5 seconds. The default value is 10 seconds.

Command Default

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:

```
Router(config)# 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 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.

Command Default

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:

```
Router(config)# interface ethernet 0
Router(config-if)# 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.

Command Default

Router forwarding is 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.

```
Router(config)# ip forward-protocol udp
Router(config)# interface ethernet 1
Router(config-if)# 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.

Command Default

IP broadcast flooding is 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:

```
Router(config)# 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

UDP turbo flooding is 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:

```
Router(config)# ip forward-protocol turbo-flood
Router(config)# ip forward-protocol spanning-tree
!
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.9.1.1
Router(config-if)# bridge-group 1
```

```
!
Router(config)# interface ethernet 1
Router(config-if)# ip address 10.9.1.2
Router(config-if)# bridge-group 1
!
Router(config)# 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:

```
Router(config)# 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 forwarding of User Datagram Protocol (UDP) broadcasts, including Bootstrap Protocol (BOOTP), received on an interface, use the **ip helper-address** command in interface configuration mode. To disable 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 the VPN routing and forwarding (VRF) instance and the 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 Virtual Router Group (VRG) name.

Command Default

UDP broadcasts are not forwarded.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)B	This command was modified. The **vrf** *name* keyword and argument pair and the **global** keyword were added.
12.2(15)T	This command was modified. The **redundancy** *vrg-name* keyword and argument pair 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

The **ip forward-protocol** command along with the **ip helper-address** command allows you to control broadcast packets and protocols that are forwarded.

One common application that requires helper addresses is 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 must specify the address of the BOOTP or DHCP server. If you have multiple servers, configure one helper address for each server.

The following conditions must be met for a UDP or IP packet to be able to use 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 VPN or global space that is different from the interface VPN, then the **vrf** *name* or the **global** option allows you to specify the name of the VRF or global space in which the DHCP server resides.

The **ip helper-addressvrf***name address* option uses the address associated with the VRF name regardless of the VRF of the incoming interface. If the **ip helper-addressvrf***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* command 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.

The **service dhcp** command must be configured on the router to enable IP helper statements to work with DHCP. If the command is not configured, the DHCP packets will not be relayed through the IP helper statements. The **service dhcp** command is configured by default.

Examples

The following example shows how to define an address that acts as a helper address:

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRF named host1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

The following example shows how to define an address that acts as a helper address and is associated with a VRG named group1:

```
Router(config)# interface ethernet 1/0
Router(config-if)# 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.
service dhcp	Enables the DHCP server and relay agent features on the router.

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.

Command Default

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.

Release	Modification
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:

```
Router(config)# ip icmp rate-limit unreachable 10
```

The following example turns off the previously configured rate limit:

```
Router(config)# no ip icmp rate-limit unreachable
```

The following example sets the rate limit back to the default:

```
Router(config)# no ip icmp rate-limit unreachable
```

The following example sets a logging packet threshold and time interval:

```
Router(config)# 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.

Command Default

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:

```
Router(config)# ip icmp redirect host
```

The following example sets the value back to the default, which is subnet redirects:

```
Router(config)# ip icmp redirect subnet
```

Related Commands

Command	Description
ip redirects	Enables the sending of ICMP redirect messages.

ip information-reply

To configure Cisco IOS software to 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.

Command Default

ICMP information replies are not sent.

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:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.108.1.0 255.255.255.0
Router(config-if)# ip information-reply
```

ip mask-reply

To configure Cisco IOS software to 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.

Command Default

ICMP mask reply messages are not sent.

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:

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.108.1.0 255.255.255.0
Router(config-if)# 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 size, in bytes.

Command Default

The default MTU value depends on the interface type.

Table 1: Default MTU Values by Interface Type

Interface Type	Default MTU (Bytes)
ATM	4470
Ethernet	1500
FDDI	4470
High-Speed Serial Interface High Speed Access (HSSI HSA)	4470
Serial	1500
Token Ring	4464
VRF-Aware Service Infrastructure (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.

Release	Modification
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 size that is set for the interface, the Cisco software fragments the IP packet.

When an IPsec MTU is less than 256 bytes, the crypto engine MTU is set to 256 bytes and packets greater than 256 bytes are fragmented.

For VASI interfaces that involve Ethernet type interfaces (Ethernet, Fast Ethernet, or Gigabit Ethernet), the IP MTU size of a VASI interface must be set to the same value 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 requires a long time.

Note Changing the MTU value (by using 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, then the IP MTU value is modified automatically to match the new MTU value. However, the reverse is not true; changing the IP MTU value has no effect on the MTU value.

If a dynamic virtual tunnel interface (VTI) configured with an IP MTU causes encapsulating security payload (ESP) fragmentation, clear and re-establish the encryption session.

When a loopback interface is used as the VTI tunnel source, you must manually configure the **ip mtu** command. This is because the IPsec encapsulation bytes are calculated based on the outgoing physical interface.

MTU Size in an IPsec Configuration

In an IPsec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, the MTU value is automatically overwritten and given a value of 256 bytes.

MTU Size in Cisco ME 3600X Series Ethernet Access Switches

In Cisco ME 3600X Series Ethernet Access Switches, you can configure seven unique MTU sizes on router and switchport interfaces and eight unique sizes on VLAN interfaces. This does not include the default size of 1500.

Examples

The following example shows how to set the maximum IP packet size for the first serial interface to 300 bytes:

```
Device(config)# interface serial 0
Device(config-if)# ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the 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.

Command Default

ICMP redirect messages are sent.

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:

```
Router(config)# interface ethernet 0
Router(config-if)# ip redirects
```

Related Commands

Command	Description
ip default-gateway	Defines a default gateway (router) when IP routing is disabled.

Command	Description
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.

The table below 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.

SCTP Chunk Type	SCTP Chunk Number	Description
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.
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:

```
Router(config)# 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 tcp adjust-mss through ip wccp web-cache accelerated

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP synchronize/start (SYN) packets that go 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 modified. 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, the host 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 size is 1460 bytes, when the default MTU of the containing IP datagram 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 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 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 that pass through the router.

In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. This value and the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte IP datagram that matches the MTU size of 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.

Command Default

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:

```
Router(config)# 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:

```
Router(config)# 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

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 keepalive

To configure TCP keepalive parameters, use the **ip tcp keepalive** command in global configuration mode. To restore the default configuration, use the **no** form of this command.

ip tcp keepalive {**interval** *seconds*| **retries** *retry-number*}

no ip tcp keepalive

Syntax Description

interval *seconds*	Specifies the TCP keepalive interval in seconds. The range is from 1 to 7200. The default value is 60 seconds.
retries *retry-number*	Specifies the number of TCP keepalive retries. The range is from 1 to 10. The default value is 4.

Command Default

TCP keepalive parameters are configured with their default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

- This command can be used only on TTY and vty applications.
- The keepalive probing can be enabled by configuring the **service tcp-keepalives-in** and **service tcp-keepalives-out** commands. However, the parameters of the **ip tcp keepalive** command can be modified without configuring these commands.

Examples

The following example shows how to set the TCP keepalive interval as 23:

```
Device# configure terminal
Device(config)# ip tcp keepalive interval 23
```

Related Commands

Command	Description
configure replace	Replaces the current running configuration with a saved Cisco IOS configuration file.
service tcp-keepalives-in	Generates keepalive packets on the idle incoming network connection.
services tcp-keepalives-out	Generates keepalive packets on the idle outgoing network connections.

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.

Command Default

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:

```
Router(config)# 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.

Command Default

Path MTU Discovery is 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:

```
Router(config)# 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.

Command Default

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:

```
Router(config)# 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.

Command Default

TCP selective acknowledgment is not enabled.

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:

```
Router(config)# 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.

Command Default

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:

```
Router(config)# 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.

Command Default

TCP time stamp is 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:

```
Router(config)# 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:

```
Router(config)# 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.

Command Default

ICMP unreachable messages are not 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:

```
Router(config)# interface ethernet 0
Router(config-if)# 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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

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:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# 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 or IPv6 route in a specific VPN virtual routing and forwarding (VRF) table, use the **ip vrf** or **ipv6 vrf** command in tracking configuration mode. To remove the tracking of the route, use the **no** form of this command.

{**ip**| **ipv6**} **vrf** *vrf-name*

no {**ip**| **ipv6**} **vrf** *vrf-name*

Syntax Description

ip	Tracks an IP route.
ipv6	Tracks an IPv6 route.
vrf-name	Name assigned to a VRF.

Command Default

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.
15.3(3)M	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

This command is available for all IP-route or IPv6 -route tracked objects that are tracked by the **track route** command in global configuration mode. Use this command to track a route that belongs to a specific VPN.

Examples

In the following example, the route associated with the VRF1 table is tracked:

```
Router(config)# track 1 ip route 10.0.0.0 255.0.0.0 metric threshold
Router(config-track)# ip vrf VRF1
Router(config-track)# rd 100:1
```

```
Router(config-track)# 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
```

In the following example, the IPv6 route associated with the VRF2 table is tracked:

```
Router(config)# track 6 ipv6 route 2001:DB8:0:ABCD::1/10 metric threshold
Router(config-track)# ipv6 vrf VRF2
```

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 is one of the services. The maximum number of services, including those assigned with the *service-number* argument, is 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 used in the cache cluster, 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.
mode open	(Optional) Identifies the service as open. This is the default service mode.
mode closed	(Optional) Identifies the service as closed.

group-address *multicast-address*	(Optional) Specifies the 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) Specifies the 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) in length that specifies the access list.
group-list *access-list*	(Optional) Specifies the 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) Specifies the 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.

Release	Modification
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.
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument pair were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. 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. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a router to enable or disable 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 also sent to the group address. 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:

- 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 in length. 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 packets to external intermediate devices for the purpose of applying feature processing are not available within Cisco IOS software, packets for the application must be blocked 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 be used only 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 the 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 service list definitions conflict, 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 access control list (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 group listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for WCCP.
ip wccp redirect exclude in	Enables redirection exclusion on an interface.
ip wccp redirect out	Configures redirection on an interface in the outgoing direction.

Command	Description
ip wccp version	Specifies which version of WCCP you want to use on your router.
show ip wccp	Displays global statistics related to WCCP.

ip wccp check acl outbound

To check the access control list (ACL) for egress interfaces for packets redirected by the Web Cache Communication Protocol (WCCP), use the **ip wccp check acl outbound** command in global configuration mode. To disable the outbound check for redirected packets, 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.

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 outbound-acl-check** command.

Examples

The following example shows how to configure a router to check the ACL for the egress interfaces for inbound packets that are redirected by 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 ACL for egress interfaces for packets redirected by 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.

Command Default

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 access control list (ACL) and by the priority value of the service.

An interface can be configured 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 that 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 want 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 (VRF) instance 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.

Command Default

No interface is configured to enable the reception of IP multicast packets for WCCP.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(17d)SXB	Support was added for the Supervisor Engine 2.
12.2(18)SXD1	Support was added for 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.

Release	Modification
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelin

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 value for the *service-number* argument 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.

Note the following requirements on routers that are to be members of a service group when IP multicast is used:

- 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 wants 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 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 multicast-routing	Enables IP multicast routing.
ip wccp	Enables support of the WCCP service for participation in a service group.
ip wccp redirect	Enables WCCP redirection on an interface.
ipv6 multicast-routing	Enables multicast routing.

ip wccp outbound-acl-check

To check the access control list (ACL) for egress interfaces for packets redirected by Web Cache Communication Protocol (WCCP) , use the **ip wccp outbound-acl-check** command in global configuration mode. To disable the outbound check for redirected packets, 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 check the ACL for the egress interfaces for inbound packets that are redirected by 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 ACL for egress interfaces for packets redirected by 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 the 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 (VRF) instance 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 was added for the Cisco 7600 series router Supervisor Engine 2.
12.2(18)SXD1	Support was added for the Cisco 7600 series router Supervisor Engine 720.

Release	Modification
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.
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.
12.2(50)SY	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding on the content engine interface, and specify the **ip wccp web-cache redirect out** command. 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. 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. Packets that match the criteria will be redirected.

The **ip wccp redirect out** command allows you to configure the WCCP redirection check at an outbound interface.

Tip 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 can affect the **ip wccp redirect exclude in** command behavior. (These commands have opposite functions.) If you have the **ip wccp redirect exclude in** command set on an interface and you subsequently configure the **ip wccp redirect in** command, the **ip wccp redirect exclude in** command will be overridden. The opposite is also true: Configuring the **ip wccp redirect exclude in** command will override the **ip wccp redirect in** command.

Examples

In the following configuration, the multilink interface is configured to prevent the bypassing of NAT when Cisco Express Forwarding 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	Enables support of the specified WCCP service for participation in a service group.
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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

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 and to allow for the use of the WCCPv2 packet return feature.

Examples

In the following example, packets arriving on Ethernet interface 0 are excluded from all WCCP redirection checks:

```
Router(config)# interface ethernet 0
Router(config-if)# ip wccp redirect exclude in
```

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 (VRF) instance 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. If a loopback interface does not exist, then the interface that WCCP uses as the preferred router ID and GRE source address cannot be specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

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, the configuration is ignored and 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.

In the error case above, the source interface for the router ID will be selected automatically.

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.

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 is enabled.

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.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Configuring this command does not have any impact on Cisco ASR 1000 Series Aggregation Services Routers because these routers support only WCCPv2. WCCPv2 is enabled by default on Cisco ASR 1000 Series Aggregation Services 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:

```
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.

Command Default

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.

M through P

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.

Command Default

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.

Command Default

Reflexive TCP/UDP shortcuts in TCAM are not enabled.

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.

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.
12.2(50)SY	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, 15.1(1)S and 12.2(50)SY, 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.

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.

sctp through show ip sctp statistics

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

SCTP configuration commands cannot be entered.

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.

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#
```

The table below 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.

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 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
```

The table below describes the significant fields shown in the display.

Table 4: 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
```

The table below describes the fields shown in the display.

Table 5: 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.

Command Default

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
```

The table below describes the significant fields shown in the displays.

Table 6: 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).

Field	Description
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 inuser 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 destinationIP 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.

Release	Modification
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
```

The table below describes the significant fields shown in the display.

Table 7: 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.

Field	Description
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)
```

The table below describes the significant fields shown in the display.

Table 8: 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.

Field	Description
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
```

The table below describes the significant fields shown in the display.

Table 9: 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.

Field	Description
Wildcard Denies	Protocol violations.
Wildcard Drops	Not enough memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.
Bytes Throughput	Number of bytes passed through all wildcards.
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.

The table below describes significant fields shown in the display.

Table 10: 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.

Field	Description
Interest Addr	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.
Interest Tickle	List of packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.
Advertise Dest Address	Destination address.
Match Fragments	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 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
```

The table below describes the significant fields shown in the display.

Table 11: show ip helper-address Field Descriptions

Field	Description
Interface	Name of the interface.
Helper-Address	IP addresses in the helper-address table.
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* 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.

Command Default

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
```

The table below describes the significant fields shown in the display.

Table 12: 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
```

The table below describes the significant fields shown in the display.

Table 13: 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
```

The table below describes the significant fields shown in the display.

Table 14: show ip sctp association parameters Field Descriptions

Field	Description
AssocID	SCTP association identifier.
Context	Internal upper-layer handle.

Field	Description
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.
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.

Field	Description
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 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.

Command	Description
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
```

The table below describes the significant fields shown in the display.

Table 15: 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.

Command	Description
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.

Command	Description
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 sockets through show sockets

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
```

The table below describes the significant fields shown in the display.

Table 16: 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
```

The table below describes the significant fields shown in the display.

Table 17: 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.
efficiencyimprovement 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.
rxslots	Total number of receive slots.

Field	Description
txslots	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.
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

Command	Description
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)*.

Release	Modification
15.1(4)M	This command was modified. The optional **interface** keyword and associated *type* and *tynumber* arguments were added. 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
```

The following is sample output from the **show ip traffic** command for Ethernet interface 0/0:

```
Router# show ip traffic interface ethernet 0/0

Ethernet0/0 IP-IF statistics :
  Rcvd:  99 total, 9900 total_bytes
         0 format errors, 0 hop count exceeded
         0 bad header, 0 no route
         0 bad destination, 0 not a router
         0 no protocol, 0 truncated
         0 forwarded
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
         0 discards, 99 delivers
  Sent:  99 total, 9900 total_bytes 0 discards
         99 generated, 0 forwarded
         0 fragmented into, 0 fragments, 0 failed
  Mcast: 0 received, 0 received bytes
         0 sent, 0 sent bytes
  Bcast: 0 received, 0 sent
```

Examples

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
```

The table below describes the significant fields shown in the display.

Table 18: show ip traffic Field Descriptions

Field	Description
format errors	Indicates a gross error in the packet format, such as an impossible Internet header length.
bad hop count	Occurs when a packet is discarded because its time-to-live (TTL) field was decremented to zero.
encapsulation failed	Usually indicates that the router had no ARP request entry and therefore did not send a datagram.
no route	Counted when the Cisco IOS software discards a datagram 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 IPv4 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 [**all**] **[capabilities] [summary]** [**interfaces** [**cef**| **counts**| **detail**]] [**vrf** *vrf-name*] [{**web-cache**| *service-number*} **[assignment] [clients] [counters] [detail] [service] [view]**]

Syntax Description

all	(Optional) Displays statistics for all known services.
capabilities	(Optional) Displays WCCP platform capabilities information.
summary	(Optional) Displays a summary of WCCP services.
interfaces	(Optional) Displays WCCP redirect interfaces.
cef	(Optional) Displays Cisco Express Forwarding interface statistics, including the number of input, output, dynamic, static, and multicast services.
counts	(Optional) Displays WCCP interface count statistics, including the number of Cisco Express Forwarding and process-switched output and input packets redirected.
detail	(Optional) Displays WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance associated with a service group to display.
web-cache	(Optional) Displays statistics for the web cache service.
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.
assignment	(Optional) Displays service group assignment information.

clients	(Optional) Displays detailed information about the clients of a service, including all per-client information. No per-service information is displayed.
counters	(Optional) Displays traffic counters.
detail	(Optional) Displays detailed information about the clients of a service, including all per-client information. No per-service information is displayed. Assignment information is also displayed.
service	(Optional) Displays detailed information about a service, including the service definition and all other per-service information.
view	(Optional) Displays other members of a particular service group, or all service groups, that have or have not been detected.

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 and Cisco Express Forwarding) when WCCP is enabled.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was added for the Supervisor Engine 2.
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.

Release	Modification
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**, **capabilities**, **clients**, **counters**, **full**, **id** *ip-address*, **service**, **summary**, and **vrf** *vrf-name*. The output was modified to display information about the WCCP client timeout interval and the redirect assignment timeout.
12.2(50)SY	This command was modified. The **summary** keyword and the **vrf** *vrf-name* keyword and argument pair were added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

Use the **clear ip wccp** command to reset all WCCP counters.

Use the **show ip wccp** *service-number* **detail** command to display information about the WCCP client timeout interval and the redirect assignment timeout interval if those intervals are not set to their default value of 10 seconds.

Use the **show ip wccp summary** command to display the configured WCCP services and a summary of their current state.

On Cisco ASR 1000 Series Aggregation Services 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** *service-number* **clients**
- **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 clients**
- **show ip wccp web-cache service**
- **show ip wccp summary**

Examples

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:                   209.165.200.225

    Service Identifier: 90
        Protocol Version:                    2.00
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        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 GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
```

The table below describes the significant fields shown in the display.

Table 19: 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.

Field	Description
Total Packets Redirected	Total number of packets redirected by the router.
Service mode	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 GRE Bypassed Packets Received	The number of generic routing encapsulation (GRE) packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

Examples

The following is sample output from the **show ip wccp** *service-number* **view** command for service group 1:

```
Router# show ip wccp 90 view

WCCP Routers Informed of:
 209.165.200.225
 209.165.200.226
WCCP Clients Visible
 209.165.200.227
 209.165.200.228
```

```
WCCP Clients 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.

The table below describes the significant fields shown in the display.

Table 20: 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.

Examples

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: 209.165.200.226
 Protocol Version: 2.0
 State:                    Usable
        Redirection:             L2
        Packet Return:           L2
        Assignment:              MASK
        Connect Time:            6d20h
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          32 of 64 (50.00%)
        Assigned masks/values:   1/32

        Mask  SrcAddr    DstAddr    SrcPort DstPort
        ----  -------    -------    ------- -------
        0000: 0x00000000 0x00001741 0x0000  0x0000

        Value SrcAddr    DstAddr    SrcPort DstPort
        ----- -------    -------    ------- -------
        0000: 0x00000000 0x00000001 0x0000  0x0000
        0001: 0x00000000 0x00000041 0x0000  0x0000
        0002: 0x00000000 0x00000101 0x0000  0x0000
        0003: 0x00000000 0x00000141 0x0000  0x0000
        0004: 0x00000000 0x00000201 0x0000  0x0000
        0005: 0x00000000 0x00000241 0x0000  0x0000
        0006: 0x00000000 0x00000301 0x0000  0x0000
        0007: 0x00000000 0x00000341 0x0000  0x0000
```

```
0008: 0x00000000 0x00000401 0x0000  0x0000
0009: 0x00000000 0x00000441 0x0000  0x0000
0010: 0x00000000 0x00000501 0x0000  0x0000
0011: 0x00000000 0x00000541 0x0000  0x0000
0012: 0x00000000 0x00000601 0x0000  0x0000
0013: 0x00000000 0x00000641 0x0000  0x0000
0014: 0x00000000 0x00000701 0x0000  0x0000
0015: 0x00000000 0x00000741 0x0000  0x0000
0016: 0x00000000 0x00001001 0x0000  0x0000
0017: 0x00000000 0x00001041 0x0000  0x0000
0018: 0x00000000 0x00001101 0x0000  0x0000
0019: 0x00000000 0x00001141 0x0000  0x0000
0020: 0x00000000 0x00001201 0x0000  0x0000
0021: 0x00000000 0x00001241 0x0000  0x0000
0022: 0x00000000 0x00001301 0x0000  0x0000
0023: 0x00000000 0x00001341 0x0000  0x0000
0024: 0x00000000 0x00001401 0x0000  0x0000
0025: 0x00000000 0x00001441 0x0000  0x0000
0026: 0x00000000 0x00001501 0x0000  0x0000
0027: 0x00000000 0x00001541 0x0000  0x0000
0028: 0x00000000 0x00001601 0x0000  0x0000
0029: 0x00000000 0x00001641 0x0000  0x0000
0030: 0x00000000 0x00001701 0x0000  0x0000
0031: 0x00000000 0x00001741 0x0000  0x0000


WCCP Client ID:          192.0.2.11
Protocol Version:        2.01
State:                   Usable
Redirection:             L2
Packet Return:           L2
Assignment:              MASK
Connect Time:            6d20h
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Mask Allotment:          32 of 64 (50.00%)
Assigned masks/values:   1/32

Mask  SrcAddr    DstAddr    SrcPort DstPort
----  -------    -------    ------- -------
0000: 0x00000000 0x00001741 0x0000  0x0000

Value SrcAddr    DstAddr    SrcPort DstPort
----- -------    -------    ------- -------
0000: 0x00000000 0x00000000 0x0000  0x0000
0001: 0x00000000 0x00000040 0x0000  0x0000
0002: 0x00000000 0x00000100 0x0000  0x0000
0003: 0x00000000 0x00000140 0x0000  0x0000
0004: 0x00000000 0x00000200 0x0000  0x0000
0005: 0x00000000 0x00000240 0x0000  0x0000
0006: 0x00000000 0x00000300 0x0000  0x0000
0007: 0x00000000 0x00000340 0x0000  0x0000
0008: 0x00000000 0x00000400 0x0000  0x0000
0009: 0x00000000 0x00000440 0x0000  0x0000
0010: 0x00000000 0x00000500 0x0000  0x0000
0011: 0x00000000 0x00000540 0x0000  0x0000
0012: 0x00000000 0x00000600 0x0000  0x0000
0013: 0x00000000 0x00000640 0x0000  0x0000
0014: 0x00000000 0x00000700 0x0000  0x0000
0015: 0x00000000 0x00000740 0x0000  0x0000
0016: 0x00000000 0x00001000 0x0000  0x0000
0017: 0x00000000 0x00001040 0x0000  0x0000
0018: 0x00000000 0x00001100 0x0000  0x0000
0019: 0x00000000 0x00001140 0x0000  0x0000
0020: 0x00000000 0x00001200 0x0000  0x0000
0021: 0x00000000 0x00001240 0x0000  0x0000
0022: 0x00000000 0x00001300 0x0000  0x0000
0023: 0x00000000 0x00001340 0x0000  0x0000
0024: 0x00000000 0x00001400 0x0000  0x0000
```

```
0025: 0x00000000 0x00001440 0x0000  0x0000
0026: 0x00000000 0x00001500 0x0000  0x0000
0027: 0x00000000 0x00001540 0x0000  0x0000
0028: 0x00000000 0x00001600 0x0000  0x0000
0029: 0x00000000 0x00001640 0x0000  0x0000
0030: 0x00000000 0x00001700 0x0000  0x0000
0031: 0x00000000 0x00001740 0x0000  0x0000
```

The table below describes the significant fields shown in the display.

Table 21: show ip wccp service-number detail Field Descriptions

Field	Description
Protocol Version	Indicates whether WCCPv1 or WCCPv2 is enabled.
State	Indicates whether the WCCP client is operating properly and can be contacted by a router and other clients in the service group. When a WCCP client has an incompatible message interval setting, the state of the client is shown as "NOT Usable," followed by a status message describing the reason why the client is not usable.
Redirection	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Assignment	Indicates the load-balancing method used. WCCP uses HASH or MASK assignment.
Connect Time	The amount of time the client has been connected to the router.
Redirected Packets	The number of packets that have been redirected to the content engine.

Examples

The following example displays WCCP client information and WCCP router statistics that include the type of services:

```
Router# show ip wccp 91 clients

WCCP Client information:
 WCCP Client ID: 10.1.1.14
 Protocol Version: 2.0
 State:                  Usable
        Redirection:             L2
        Packet Return:           L2
        Assignment:              MASK
        Connect Time:            6d20h
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Mask Allotment:          32 of 64 (50.00%)
```

```
WCCP Client ID:          192.0.2.11
Protocol Version:        2.01
State:                   Usable
Redirection:             L2
Packet Return:           L2
Assignment:              MASK
Connect Time:            6d20h
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Mask Allotment:          32 of 64 (50.00%)
```

The table below describes the significant fields shown in the display.

Table 22: show ip wccp service-number clients Field Descriptions

Field	Description
Protocol Version	Indicates whether WCCPv1 or WCCPv2 is enabled.
State	Indicates whether the WCCP client is operating properly and can be contacted by a router and other clients in the service group. When a WCCP client has an incompatible message interval setting, the state of the client is shown as "NOT Usable," followed by a status message describing the reason why the client is not usable.
Redirection	Indicates the redirection method used. WCCP uses GRE or L2 to redirect IP traffic.
Assignment	Indicates the load-balancing method used. WCCP uses HASH or MASK assignment.
Connect Time	The amount of time (in seconds) the client has been connected to the router.
Redirected Packets	The number of packets that have been redirected to the content engine.

Examples

The following is sample output from the **show ip wccp interfaces** command:

```
Router# show ip wccp interfaces

IPv4 WCCP interface configuration:
    FastEthernet2/1
        Output services: 0
        Input services:  1
        Mcast services:  0
        Exclude In:      FALSE
```

The table below describes the significant fields shown in the display.

Table 23: 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.
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

Examples

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:                   209.165.200.225

    Service Identifier: web-cache
        Protocol Version:                    2.00
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        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 GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
        GRE tunnel interface:                Tunnel0
```

The table below describes the significant fields shown in the display.

Table 24: show ip wccp web-cache Field Descriptions

Field	Description
Service Identifier	Indicates which service is detailed.
Protocol Version	Indicates whether WCCPv1 or WCCPv2 is enabled.
Number of Service Group Clients	Number of clients using the router as their home router.

Field	Description
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.
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.

Examples

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:                  0
     CEF:                      0
   Non-Redirected Packets:
     Action - Forward:
       Reason - no assignment:
         Process:              0
         CEF:                  0
     Action - Ignore (forward):
       Reason - redir ACL check:
         Process:              0
         CEF:                  0
     Action - Discard:
       Reason - closed services:
         Process:              0
         CEF:                  0
   GRE Bypassed Packets:
     Process:                  0
```

```
    CEF:                        0
  GRE Bypassed Packet Errors:
    Total Errors:
      Process:                  0
      CEF:                      0

  WCCP Client Counters:
    WCCP Client ID:             192.0.2.12
       Redirected Packets:
         Process:               0
         CEF:                   0
       GRE Bypassed Packets:
         Process:               0
         CEF:                   0

    WCCP Client ID:             192.0.2.11
       Redirected Packets:
         Process:               0
         CEF:                   0
       GRE Bypassed Packets:
         Process:               0
         CEF:                   0
```

The table below describes the significant fields shown in the display.

Table 25: 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.

Examples

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:          209.165.200.225
        Protocol Version:        2.0
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w5d
        Redirected Packets:
          Process:               0
          CEF:                   0
        GRE Bypassed Packets:
          Process:               0
          CEF:                   0
        Hash Allotment:          128 of 256 (50.00%)
        Initial Hash Info:       00000000000000000000000000000000
                                 00000000000000000000000000000000
        Assigned Hash Info:      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                                 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

        WCCP Client ID:          192.0.2.11
        Protocol Version:        2.01
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Connect Time:            1w5d
```

```
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Hash Allotment:         128 of 256 (50.00%)
        Initial Hash Info:      00000000000000000000000000000000
                                00000000000000000000000000000000
        Assigned Hash Info:     55555555555555555555555555555555
                                55555555555555555555555555555555
```

The table below describes the significant fields shown in the display.

Table 26: 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.
Protocol Version	The version of WCCP being used by the cache engine in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Connect Time	The amount of time the cache engine has been connected to the router.
Redirected Packets	The number of packets that have been redirected to the cache engine.

Examples

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 Client information:
        WCCP Client ID:         209.165.200.225
        Protocol Version:       2.01
        State:                  Usable
        Redirection:            GRE
        Packet Return:          GRE
        Assignment:             HASH
        Connect Time:           1w5d
        Redirected Packets:
          Process:              0
          CEF:                  0
        GRE Bypassed Packets:
          Process:              0
          CEF:                  0
        Hash Allotment:         128 of 256 (50.00%)
        Initial Hash Info:      00000000000000000000000000000000
                                00000000000000000000000000000000
        Assigned Hash Info:     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
                                AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

        WCCP Client ID:         209.165.200.226
```

```
Protocol Version:        2.01
State:                   Usable
Redirection:             GRE
Packet Return:           GRE
Assignment:              HASH
Connect Time:            1w5d
Redirected Packets:
  Process:               0
  CEF:                   0
GRE Bypassed Packets:
  Process:               0
  CEF:                   0
Hash Allotment:          128 of 256 (50.00%)
Initial Hash Info:       00000000000000000000000000000000
                         00000000000000000000000000000000
Assigned Hash Info:      55555555555555555555555555555555
                         55555555555555555555555555555555
```

The table below describes the significant fields shown in the display.

Table 27: 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.
Protocol Version	The version of WCCP that is being used by the router in the service group.
State	Indicates whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.
Connect Time	The amount of time the cache engine has been connected to the router.
Hash Allotment	The percent of buckets assigned to the current cache engine. Both a value and a percent figure are displayed.
Initial Hash Info	The initial state of the hash bucket assignment.
Assigned Hash Info	The current state of the hash bucket assignment.
Redirected Packets	The number of packets that have been redirected to the cache engine.
GRE Bypassed Packets	The number of packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

Examples

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
        Flags:          0x00000512
          Hash:         DstIP
          Alt Hash:     SrcIP SrcPort
          Ports used:   Destination
        Ports:          80
```

Examples

The following example displays information about 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: 209.165.200.225):
web-cache   2         1         HASH        GRE        GRE
90          0         0         HASH/MASK   GRE/L2     GRE/L2
```

The table below describes the significant fields shown in the display.

Table 28: show ip wccp summary 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.
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 ip wccp *service-number* **detail**	Displays information about the WCCP client timeout interval and the redirect assignment timeout interval if those intervals are not set to their default value of 10 seconds.
show ip wccp summary	Displays the configured WCCP services and a summary of their current state.
show platform software wccp	Displays global statistics related to WCCP on Cisco ASR 1000 Series Aggregation Services Routers.

show ip wccp global counters

To display IPv4 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 counters** command displays counters for packets that are processed in software. These counters are always zero on the Cisco ASR 1000 Series Aggregation Services 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
```

The table below describes the significant fields shown in the display.

Table 29: show ip wccp global counters Field Descriptions

Field	Description
CEF (In)	Number of incoming Cisco Express Forwarding packets
CEF (Out)	Number of outgoing Cisco Express Forwarding packets.

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 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* **[ipv6]**

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.
ipv6	(Optional) Specifies the WCCP IPv6 service.

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.
Cisco IOS XE Release 3.10S	This command was modified. The **ipv6** keyword was added.

Examples

The following is a sample output of 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
```

The table below describes the significant fields shown in the display:

Table 30: 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.
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).

Examples

The following is a sample output of the **show platform hardware qfp active feature wccp ipv6** command:

```
Router# show platform hardware qfp active feature wccp service id 61 ipv6

Service ID: 61
Service Type: 1
Service Priority: 34
Assign Method: 1
Hash key: 0x51
Hash buckets ppe address: 0x8bceb600
Mode: Open
State: Active
Number of Caches in this service: 1
  ce index: 0
  cache_id : 11
  Cache ip addr : 0x20010001
  Cache cfg ppe addr : 0x8bcab200
  Cache oce ppe addr : 0x891a7670
  Cache state ppe addr : 0x8bcfd288
Number of interfaces using this service: 1
  Interface: GigabitEthernet0/0/0.1
  cpp-if-h: 12
  Dir: 0
  pal-if-h: 15
  uidb sb ppe addr: 0x8bd308e0
```

The table below describes the significant fields shown in the display:

Table 31: show platform hardware qfp active feature wccp ipv6 Field Descriptions

Field	Description
Service ID	Service group number (0 for webcache and 1 to 254 for dynamic services).
Service Type	Specifies the WCCP service type, whether standard or dynamic.
Service Priority	Priority of the service group.
Assign Method	Indicates the load-balancing method used (1 for hash and 0 for mask).
Hash key	Identifies the hash value.
Hash buckets ppe address	Specifies the PPE address of the hash bucket.
Mode	Specifies whether the service group has been defined as an open service group (default value) or closed service group.
State	Specifies the current WCCP state.
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* **ipv6 counters**| [*slot* { **active**| **standby** }[*service-number* { **access-list**| **ipv6** }| **cache-info**| **interface**| **statistics**| **web-cache** { **access-list**| **ipv6** }]| [**vrf** *vrf-identifier* {*service-number* { **access-list**| **ipv6** }| **web-cache** { **access-list**| **ipv6** }}]]| **interface counters**| **statistics**| [**vrf** *vrf-identifier* {*service-number* **ipv6 counters**| **web-cache ipv6 counters**}]| **web-cache ipv6 counters**]

Syntax Description

service-number	(Optional) Displays information for a dynamically defined service. The service number can be from 0 to 254.
ipv6	(Optional) Specifies the IPv6 service.
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
active	(Optional) Specifies an active instance.
standby	(Optional) Specifies a standby instance.
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.
Cisco IOS XE Release 3.10S	This command was modified. The **active**,**standby,** and **ipv6** keywords were 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 a sample output of 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
.
.
.
```

The following is a sample output of the **show platform software wccp ipv6 counters** command:

```
Router# show platform software wccp 61 ipv6 counters

Service Group (1, 61, 0) counters
        Unassigned count = 0
        Dropped due to closed service count = 0
        Bypass count = 0
        Bypass failed count = 0
        Denied count = 0
        Redirect count = 4
  CE = 2001:1:100::105, obj_id = 213, Redirect Packets = 4
```

The table below describes the significant fields shown in the display.

Table 32: show platform software wccp counters Field Descriptions

Field	Description
Service Group (1, 61,0) 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 a sample output of 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
```

The table below describes the significant fields shown in the display.

Table 33: 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 a sample output of 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
```

The table below describes the significant fields shown in the display.

Table 34: 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
```

The table below describes the significant fields shown in the display.

Table 35: 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.

The following are sample outputs from the **show platform software wccp** *slot* **active** *service-number* **ipv6** command:

```
Router# show platform software wccp RP active 61 ipv6

IPV6 Dynamic service 61
Priority: 34, Number of clients: 1
Assign Method: Hash, Fwd Method: GRE, Ret Method: GRE
L4 proto: 6, Use Source Port: No
Is closed: No


Router# show platform software wccp FP active 61 ipv6

IPV6 Dynamic service 61
Priority: 34, Number of clients: 1
Assign Method: Hash, Fwd Method: GRE, Ret Method: GRE
Is closed: No
Current ACE: 0, Pending ACE: 0
New ACE: 0, New ACE completed: No
ACL id: 0
  AOM id: 0x18a, status: created
```

The table below describes the significant fields shown in the display.

Table 36: show platform software wccp slot active service-number ipv6 Field Descriptions

Field	Description
IPV6 Dynamic service	Specifies the IPv6 Dynamic Service number.
Priority	Specifies the priority of the service group.

Field	Description
Number of clients	Specifies the number of WCCP clients.
Assign Method	Indicates the load-balancing method used (1 for hash and 0 for mask).
Fwd Method	Specifies the WCCP forward method, whether GRE or Layer 2.
Ret Method	Specifies the WCCP return method, whether GRE or Layer 2.
L4 proto	Specifies the Layer 4 protocol. Indicates that the Layer 4 part of the packet is TCP (denoted by 6).
Use Source Port	Specifies whether the service definition uses the source port.
Is closed	Specifies whether WCCP is configured as a closed service or an open service.
Current ACE	Specifies the number of Application Control Engine (ACE) items configured.
Pending ACE	Specifies the pending number of ACE items to be downloaded.
New ACE	Specifies the number of new ACE items to be downloaded.
New ACE completed	Specifies the number of new ACE items downloaded.
ACL id	Identifies the Access Control List (ACL) configured with the WCCP service.
AOM id	Specifies the asynchronous object manager identifier.
status	Specifies the WCCP state.

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
```

The table below describes the significant fields shown in the display.

Table 37: show sctp accociation 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
```

The table below describes the significant fields shown in the display.

Table 38: show sctp association list Field Descriptions

Field	Description
AssocID	SCTP association identifier.

Field	Description
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
```

The table below describes the significant fields shown in the display.

Table 39: 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.

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.

Field	Description
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.
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
```

The table below describes the significant fields shown in the display.

Table 40: 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--
```

The table below describes the significant fields shown in the displays.

Table 41: 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.
Proto	Protocol type, such as UDP, TCP, or SCTP.

Field	Description
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.

Field	Description
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 tcp through start-forwarding-agent

show tcp

To display the status of Transmission Control Protocol (TCP) connections when Cisco IOS or Cisco IOS Software Modularity images are 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

Note Example output varies between Cisco IOS software images and Cisco IOS Software Modularity software images.

Examples

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
```

The table below contains the types of flags, all possible command output enhancements, and descriptions.

Table 42: 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.

Type of Flag	Output Enhancement	Description
	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.
	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
```

The table below describes the first five lines of output shown in the above display.

Table 43: 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.

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.

Field	Description
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.
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
```

The table below describes the fields in the above lines of output.

Table 44: 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.
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.

Field	Description
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
```

The table below describes the fields shown in the display above.

Table 45: 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
```

The table below describes the significant fields shown in the output above.

Table 46: 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
```

The table below describes the significant fields shown in the last lines of the **show tcp** command output.

Table 47: 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).

Field	Description
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
```

Examples

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
```

The table below describes the significant fields shown in the display.

Table 48: 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.

Examples

The following is sample output from the **show tcp statistics** command:

```
Router# show tcp statistics

Rcvd: 210 Total, 0 no port
      0 checksum error, 0 bad offset, 0 too short
      132 packets (26640 bytes) in sequence
      5 dup packets (502 bytes)
      0 partially dup packets (0 bytes)
      0 out-of-order packets (0 bytes)
      0 packets (0 bytes) with data after window
      0 packets after close
      0 window probe packets, 0 window update packets
      0 dup ack packets, 0 ack packets with unsend data
      69 ack packets (3044 bytes)
Sent: 175 Total, 0 urgent packets
      16 control packets (including 1 retransmitted)
```

```
      69 data packets (3029 bytes)
      0 data packets (0 bytes) retransmitted
      73 ack only packets (49 delayed)
      0 window probe packets, 17 window update packets
7 Connections initiated, 1 connections accepted, 8 connections established
8 Connections closed (including 0 dropped, 0 embryonic dropped)
1 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```

The table below describes the significant fields shown in the display.

Table 49: 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.

Field	Description
Sent:	Statistics in this section refer to packets sent by the router.
Total	Total number of TCP packets sent.
urgent packets	Number of urgent packets sent.
control packets	Number of control packets (SYN, FIN, or RST) sent.
data packets	Number of data packets sent.
data packets retransmitted	Number of data packets re-sent.
ack only packets	Number of packets sent that are acknowledgments only.
window probe packets	Number of window probe packets sent.
window update packets	Number of window update packets sent.
Connections initiated	Number of connections initiated.
connections accepted	Number of connections accepted.
connections established	Number of connections established.
Connections closed	Number of connections closed.
Total rxmt timeout	Number of times 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.

Examples

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
```

The table below describes the significant fields shown in the display that are different from the above table.

Table 50: 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.

Field	Description
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.
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.

Field	Description
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.

Command Default

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 2was extended to Release 12.2(17d)SXB.

Release	Modification
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.
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.

Release	Modification
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.
12.2(50)SY	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.
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:

Command	Description
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.
show running-config	Displays the current configuration of your routing device.

Command	Description
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.

Command Default

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
```

The table below describes the significant fields shown in the display.

Table 51: 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 sla[brief]**| **timer**]

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.
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.

Release	Modification
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.
12.2(50)SY	This command was modified. The valid range for the *object-number* argument increased to 1000.
15.3(3)S	This command was modified. The output was enhanced to display IPv6 route information.
XE 3.10S	This command was modified. The output was enhanced to display IPv6 route information.

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, 15.1(1)S, and 12.2(50)SY, 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 device 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:

```
Device# 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:

```
Device# 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:

```
Device# 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:

```
Device# 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:

```
Device# show track timer

Object type   Poll Interval  Time to next poll
interface             1             0.844
ip route             15           expired
ip sla                5           expired
ipv6 route           15           expired
application           5             2.944
list                  0.500         0.88
stub                  1           expired
```

The following example shows the state of the IP SLAs tracking:

```
Device# 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:

```
Device# 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
```

The table below describes the significant fields shown in the displays.

Table 52: 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.

Field	Description
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.”

```
Device# 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:

```
Device# 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
```

The table below describes the significant fields shown in the displays.

Table 53: 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.

Field	Description
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):

```
Device# 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:

```
Device# 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:

```
Device# show track

Track 101
Interface Ethernet1/0 line-protocol
Line protocol is Down (carrier-delay)
1 change, last change 00:00:03
```

The table below describes the significant fields shown in the displays.

Table 54: 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.

The table below describes the significant fields shown in the displays.

Table 55: 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.

The following example shows sample output with respect to IPv6 routing:

```
Router# show track
Track 107
  Interface Ethernet0/0 ipv6 routing
  IPv6 routing is Down (ipv6 interface disabled)
    1 change, last change 00:03:53
  Delay up 70 secs
Track 108
  Interface Ethernet0/0 ipv6 routing
  IPv6 routing is Down (ipv6 interface disabled)
    1 change, last change 00:03:53
  Delay up 10 secs, down 30 secs
Track 111
  Interface Ethernet0/1 line-protocol
  Line protocol is Up
    1 change, last change 00:14:17
Track 601
  IPv6 route 2001:DB8::EEEE/64 metric threshold
  Metric threshold is Down (no ipv6 route)
    1 change, last change 00:10:21
  Metric threshold down 255 up 254
  First-hop interface is unknown
Track 607
  IPv6 route 2001:DB8::FFFF/64 metric threshold
  Metric threshold is Down (no ipv6 route)
    1 change, last change 00:10:21
  Metric threshold down 255 up 254
  First-hop interface is unknown
Track 608
  IPv6 route 2001:DB8::FFFF:AD45/64 metric threshold
  Metric threshold is Down (no ipv6 route)
    1 change, last change 00:10:21
  Metric threshold down 140 up 120
  First-hop interface is unknown
Track 612
  IPv6 route 2001:DB8:0000::FFFF/64 reachability
  Reachability is Down (no ipv6 route)
    1 change, last change 00:10:14
  Delay up 30 secs, down 20 secs
  First-hop interface is unknown
```

The following example shows sample output with respect to IPv6 routing in brief format:

```
Router# show track
Track Object                                  Parameter          Value  Last Change
1      application                            home-agent         Up     00:14:25
101    interface     Ethernet0/0              ip routing         Up     00:14:25
107    interface     Ethernet0/0              ipv6 routing       Down   00:04:01
108   interface     Ethernet0/0               ipv6 routing       Down   00:04:01
111   interface     Ethernet0/1               line-protocol      Up     00:14:25
```

```
201    ip route      11.0.0.1/8              metric threshold   Down   00:14:25
211   ip route      21.0.0.1/8              reachability       Down   00:14:25
301    ip sla        1                       reachability       Down   00:14:25
302    ip sla        1                       reachability       Down   00:14:25
311    ip sla        1                       state              Down   00:14:25
312    ip sla        1                       state              Down   00:14:25
403    list                                  boolean            Down   00:14:25
413    list                                  boolean            Down   00:14:25
501   Stub-object  Undefined                                    Up     00:11:01
502   Stub-object  Undefined                                    Down   00:11:01
503    Stub-object  Undefined                                   Down   00:11:01
601    ipv6 route   2001:DB8::EEEE/64       metric threshold   Down   00:10:29
607    ipv6 route   2001:DB8::FFFF/64       metric threshold   Down   00:10:29
608    ipv6 route   2001:DB8::FFFF:AD45/64  metric threshold   Down   00:10:29
612    ipv6 route   2001:DB8:0000::FFFF/64  reachability       Down   00:10:22
```

Related Commands

Command	Description
showtrack resolution	Displays the resolution of tracked parameters.
track interface	Configures an interface to be tracked and enters tracking configuration mode.
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)
```

The table below describes the significant fields shown in the display.

Table 56: 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 wccp

To display all (IPv4 and IPv6) Web Cache Communication Protocol (WCCP) global configuration and statistics, use the **show ipv6 wccp** command in user EXEC or privileged EXEC mode.

show wccp [**[all] [capabilities] [summary]** [**interfaces**[**cef**| **counts**| **detail**]][**vrf** *vrf-name*][{**web-cache**| *service-number*}]]

Syntax Description

summary	(Optional) Displays a summary of WCCP services.
capabilities	(Optional) Displays WCCP platform capabilities information.
vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) instance 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) Displays WCCP redirect interfaces.
cef	(Optional) Displays Cisco Express Forwarding interface statistics, including the number of input, output, dynamic, static, and multicast services.
counts	(Optional) Displays WCCP interface count statistics, including the number of Cisco Express Forwarding and process-switched output and input packets redirected.
detail	(Optional) Displays WCCP interface configuration statistics, including the number of input, output, dynamic, static, and multicast services.
web-cache	(Optional) Displays statistics for the web cache service.
all	(Optional) Displays statistics for all known services.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

Use the **clear wccp** command to reset all WCCP counters.

Use the **show wccp** *service-number* **detail** command to display information about the WCCP client timeout interval and the redirect assignment timeout interval if those intervals are not set to their default value of 10 seconds.

Use the **show wccp summary** command to show the configured WCCP services and a summary of their current state.

Examples

This section contains examples and field descriptions for the following forms of this command:

- **show wccp** *service-number* (service mode displayed)
- **show wccp interfaces**
- **show wccp web-cache**

Examples

The following is sample output from the **show wccp** *service-number* command:

```
Router# show wccp 61

Global WCCP information:
    Router information:
        Router Identifier:                   2001:DB8:100::1

    Service Identifier: 61
        Protocol Version:                    2.01
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        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 GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
```

The table below describes the significant fields shown in the display.

Table 57: show 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.
Total Packets s/w Redirected	Total number of packets redirected by the router.
Service mode	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.

Field	Description
Total Bypassed Packets Received	The number of packets that have been bypassed. Process and Cisco Express Forwarding are switching paths within Cisco IOS software.

Examples

The following is sample output from the **show wccp interfaces** command:

```
Router# show ipv6 wccp interfaces

IPv4 WCCP interface configuration:
    FastEthernet2/1
        Output services: 0
        Input services:  1
        Mcast services:  0
        Exclude In:      FALSE

IPv6 WCCP interface configuration:
    FastEthernet2/1
        Output services: 1
        Input services:  2
        Mcast services:  0
        Exclude In:      FALSE
```

The table below describes the significant fields shown in the display.

Table 58: show 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.
Mcast services	Indicates the number of multicast services configured on the interface.
Exclude In	Displays whether traffic on the interface is excluded from redirection.

Examples

The following is sample output from the **show wccp web-cache** command:

```
Router# show ipv6 wccp web-cache

IPv4 Global WCCP information:
    Router information:
        Router Identifier:                   203.0.113.1

    Service Identifier: web-cache
        Protocol Version:                    2.01
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
```

```
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        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 GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
        GRE tunnel interface:                Tunnel0

IPv6 Global WCCP information:
    Router information:
        Router Identifier:                   2001:DB8:100::1

    Service Identifier: web-cache
        Protocol Version:                    2.01
        Number of Service Group Clients:     2
        Number of Service Group Routers:     1
        Total Packets Redirected:            0
          Process:                           0
          CEF:                               0
        Service mode:                        Open
        Service Access-list:                 -none-
        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 GRE Bypassed Packets Received: 0
          Process:                           0
          CEF:                               0
        GRE tunnel interface:                Tunnel1
```

The table below describes the significant fields shown in the display.

Table 59: show wccp web-cache Field Descriptions

Field	Description
Protocol Version	The version of WCCP that is being used by the cache engine in the service group.
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.

Field	Description
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.
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.

Related Commands

Command	Description
clear 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.
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
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.

Command	Description
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 wccp global counters

To display all (IPv4 and IPv6) global Web Cache Communication Protocol (WCCP) information for packets that are processed in software, use the **show wccp global counters** command in user EXEC or privileged EXEC mode.

show wccp global counters

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
15.1(1)SY1	This command was integrated into Cisco IOS Release 15.1(1)SY1.

Usage Guidelines

The **show wccp global counters** command displays counters for packets that are processed in software. These counters are always zero on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example displays global WCCP information for packets that are processed in the software:

```
Router# show wccp global counters

WCCP Global Counters:
Packets Seen by WCCP
Process:   8
CEF (In):  14
CEF (Out): 0
```

The table below describes the significant fields shown in the display.

Table 60: show wccp global counters Field Descriptions

Field	Description
CEF (In)	Number of incoming Cisco Express Forwarding packets
CEF (Out)	Number of outgoing Cisco Express Forwarding packets.

Related Commands

Command	Description
clear 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.
ipv6 wccp	Enables support of the WCCP service for participation in a service group.
ipv6 wccp redirect	Enables packet redirection on an outbound or inbound interface using WCCP.
show ip interface	Lists a summary of the IP information and the status of an interface.
show wccp	Displays the WCCP global configuration and statistics.

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.

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.

Command Default

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:

```
Router(config-casa)# 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.

threshold metric through track timer

threshold metric

To set a threshold metric, use the **threshold metric** command in tracking configuration mode. To remove the threshold metric value, 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.
number	Threshold value. The range is from 0 to 255. The up threshold default is 254, and the down threshold default is 255.
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.

Command Default

No threshold metric is set.

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.
15.3(3)M	This command was integrated into Cisco IOS Release 15.3(3)M.

Usage Guidelines

This command is available only for IP-route threshold metric objects tracked by the **track ip route metric threshold** command in global configuration mode.

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 threshold metric is set to 16 for the up threshold and to 20 for the down threshold. The delay period to communicate the changes of a down event of the tracked object to the client process is set to 20 seconds.

```
Router(config)# track 1 ip route 10.22.0.0/16 metric threshold
Router(config-track)# threshold metric up 16 down 20
Router(config-track)# 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:

```
Router(config)# track 11 list threshold percentage
Router(config-track)# object 1
Router(config-track)# object 2
Router(config-track)# 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 list** *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:

```
Router(config)# track 12 list threshold weight
Router(config-track)# object 1
Router(config-track)# object 2
Router(config-track)# 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.

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.

Release	Modification
12.2(50)SY	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, 15.1(1)S and 12.2(50)SY, 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 abcd

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.

Release	Modification
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.
12.2(50)SY	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, 15.1(1)S and 12.2(50)SY, 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 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.
12.2(50)SY	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, 15.1(1)S and 12.2(50)SY, 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 track an interface 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**| **ipv6 routing**}

no track *object-number* **interface** *type number* {**line-protocol**| **ip routing**| **ipv6 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.
ipv6 routing	Tracks whether IPv6 routing is enabled, whether an IPv6 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	This 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.

Release	Modification
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 integrated into Cisco IOS Release 15.1(1)S.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.3(3)M	This command was modified. The **ipv6 routing** keyword was added.

Usage Guidelines

This command reports a state value to clients. A tracked IP or IPv6 routing object is considered up when the following criteria exist:

- IP or IPv6 routing is enabled and active on the interface.
- The state of the interface line protocol is up.
- The interface address is known. The address is configured or received through the Dynamic Host Configuration Protocol (DHCP) or IP Control Protocol (IPCP) negotiation.

Interface IP or IPv6 routing goes down when one of the following criteria exist:

- IP or IPv6 routing is disabled globally.
- The state of the interface line protocol is down.
- The interface address is unknown. The address is not configured or received through DHCP or IPCP negotiation.

A space is not required between the *type* and *number*values.

Tracking the IP or IPv6 routing state of an interface can be more useful in some situations than tracking the interface-line-protocol state, 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, which means that Link Control Protocol negotiated successfully, but IP could be down, which means that IPCP negotiation failed.

The **track interface** command supports the tracking of an interface with an IP or IPv6 address acquired through any of the following methods:

- Conventional IP address configuration
- PPP/IPCP
- DHCP
- Unnumbered interface

Examples

In the following example, the tracking process is configured to track the IP-routing capability of serial interface 1/0:

```
Router(config)# track 1 interface serial1/0 ip routing
Router(config-track)#
```

In the following example, the tracking process is configured to track the IPv6-routing capability of a GigabitEthernet interface 1/0/0:

```
Router(config)# track 1 interface GigabitEthernet 1/0/0 ipv6 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**| **ipv6**} **route** *address*/*prefix-length* {**reachability**| **metric threshold**}

no track *object-number* {**ip**| **ipv6**} **route** *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	Tracks an IP route.
ipv6	Tracks an IPv6 route.
address	IP or IPv6 subnet address to the route that is being tracked.
/*prefix-length*	Number of bits in the address prefix. A forward slash (/) is required.
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.

Release	Modification
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 integrated into Cisco IOS Release 15.1(1)S.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.3(3)M	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

A tracked IP-route or IPv6-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 for 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 the route is less than or equal to the up threshold.
- State is down if the scaled metric for the 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.

As of Cisco IOS Release 15.1(3)T, 15.1(1)S, and 12.2(50)SY, 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 depends on variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects depends on available CPU resources. Testing should be conducted 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
```

In the following example, the tracking process is configured to track the threshold metric using the default threshold metric values for an IPv6 route:

```
Router(config)# track 2 ipv6 route 2001:DB8:0:ABCD::1/10 metric threshold
```

Related Commands

Command	Description
show track	Displays HSRP tracking information.
threshold metric	Sets a threshold metric.

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.

Release	Modification
12.2(50)SY	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. The table below shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 61: Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK (all other return codes)	Up Down
Reachability	OK or over threshold (all other return codes)	Up Down

As of Cisco IOS Release 15.1(3)T, 15.1(1)S and 12.2(50)SY, 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 obje cts 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.

Release	Modification
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.
12.2(50)SY	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, 15.1(1)S, and 12.2(50)SY, 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**| **ipv6 route** | {**bgp**| **eigrp**| **isis**| **ospf**| **static**}| *resolution-value*}

no track resolution {**ip route**| **ipv6 route** | {**bgp**| **eigrp**| **isis**| **ospf**| **static**}| *resolution-value*}

Syntax Description

ip route	IP route for metric resolution for a specified track. The keywords and arguments are as follows: • **bgp —**BGP routing protocol. The *resolution-value* argument has a range from 256 to 40000000. • **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.

ipv6 route	IPv6 route for metric resolution for a specified track. The keywords and arguments are as follows: • **bgp —**BGP routing protocol. The *resolution-value* argument has a range from 256 to 40000000. The default value is 2560. • **eigrp —**EIGRP routing protocol. The *resolution-value* argument has a range from 256 to 40000000. The default value is 2560. • **isis —**ISIS routing protocol. The *resolution-value* argument has a range from 1 to 1000. The default value is 10. • **ospf —**OSPF routing protocol. The *resolution-value* argument has a range from 1 to 1562. The default value is 1. • **static —**Static route. The *resolution-value* argument has a range from 1 to 100000. The default value is 10.

Command Default

The default threshold metric 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.
15.3(3)M	This command was modified. The **ipv6 route** keyword was added.

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 of 0 to 255. The metric resolution for the specified routing

protocol is used to do the conversion. There are default values for metric resolution, but the **track resolution** command can be used to change them.

Examples

In the following example, the EIGRP routing protocol has a resolution value of 280.

```
Router(config)# 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 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.

Release	Modification
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. The table below shows the state and reachability aspects of IP SLAs operations that can be tracked.

Table 62: Comparison of State and Reachability Operations

Tracking	Return Code	Track State
State	OK (all other return codes)	Up Down
Reachability	OK or over threshold (all other return codes)	Up Down

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
Router(config)# track 1 rtr 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 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.
12.2(50)SY	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, 15.1(1)S, and 12.2(50)SY, 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 that a tracking process polls a tracked object, use the **track timer** command in global configuration mode. To reset to the default polling interval, use the **no** form of this command.

track timer {**application| interface| ip** | {**route| sla**}| **ipv6 route| list| stub-object**} {*seconds*| **msec** *milliseconds*}

no track timer {**application| interface| ip** | {**route| sla**}| **ipv6 route| list| stub-object**} {*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 route polling timer.
sla	Tracks the route polling timer.
ipv6 route	Tracks the specified IPv6 protocol.
list	Tracks the boolean list polling timer.
stub-object	Tracks the Embedded Event Manager (EEM) stub polling timer.
seconds	Polling interval, in seconds. The range is from 1 to 3000. The default for interface polling is 1 second, and the default for IP-route polling is 15 seconds.
msec *milliseconds*	Specifies the polling interval in milliseconds. The range is 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, as described in the table below:

Object	Default Polling Interval (seconds)
Application	5
Interface	1

Object	Default Polling Interval (seconds)
IP route	15
IP SLA	5
IPv6 route	15
List	1
Stub-object	1

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 were 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.
15.0(1)M	This command was modified. The **application** and **msec** keywords and the *milliseconds* argument were added.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.
15.3(3)M	This command was modified. The **ipv6** keyword was added.

Examples

In the following example, the tracking process polls the tracked interface every 3 seconds:

```
Router# configure terminal
Router(config)# track timer interface 3
```

In the following example, the tracking process polls the tracked IPv6 route every 5 seconds:

```
Router# configure terminal
Router(config)# track timer ipv6 route 5
```