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.
Cisco IOS XE 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

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 1: 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.

Field	Description
WIN 4128	Advertised window size, in bytes. In this case, the bytes are 4128.
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 2: 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 3: 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 4: show ip accounting Field Descriptions

Field	Description
Source	Source address of the packet.
Destination	Destination address of the packet.
Packets	Number of packets sent from the source address to the destination address. With the **access-violations** keyword, the number of packets sent from the source address to the destination address that violated an access control list (ACL).
Bytes	Sum of the total number of bytes (IP header and data) of all IP packets sent from the source address to the destination address. With the **access-violations** keyword, the total number of bytes sent from the source address to the destination address that violated an ACL.
ACL	Number of the access list of the last packet sent from the source to the destination that failed an access list filter.
accounting threshold exceeded...	Data for all packets that could not be entered into the accounting table when the accounting table is full. This data is combined into a single entry.

Related Commands

Command	Description
clear ip accounting	Clears the active or checkpointed database when IP accounting is enabled.

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-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.
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 5: show ip casa affinities Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Port	Destination of a given TCP connection.
Prot	Protocol of a given TCP connection.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager address that is to receive interest packets for this affinity.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of TCP packet types of interest to the services manager is interested in.
Interest Tickle	List of TCP packet types for which the services manager wants the entire packet.
Dispatch (Layer 2)	Layer 2 destination information will be modified.
Dispatch Address	Address of the real server.

Related Commands

Command	Description
forwarding-agent	Specifies the port on which the forwarding agent will listen for wildcard and fixed affinities.
show ip casa oper	Displays operational information about the forwarding agent.

show ip casa oper

To display operational information about the forwarding agent, use the **show ip casa oper** command in user EXEC or privileged EXEC mode.

show ip casa oper

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show ip casa oper** command:

```
Router# show ip casa oper
Casa is Active
  Casa control address is 10.10.20.34/32
  Casa multicast address is 239.1.1.1
  Listening for wildcards on:
    Port:1637
      Current passwd:NONE Pending passwd:NONE
      Passwd timeout:180 sec (Default)
```

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

Table 6: show ip casa oper Field Descriptions

Field	Description
Casa is Active	The forwarding agent is active.
Casa control address	Unique address for this forwarding agent.
Casa multicast address	Services manager broadcast address.
Listening for wildcards on	Port on which the forwarding agent will listen.
Port	Services manager broadcast port.
Current passwd	Current password.
Pending passwd	Password that will override the current password.
Passwd timeout	Interval after which the pending password becomes the current password.

Related Commands

Command	Description
ip casa oper	Configures the router to function as an MNLB forwarding agent.

show ip casa stats

To display statistical information about the Forwarding Agent, use the **show ip casa stats** command in user EXEC or privileged EXEC mode.

show ip casa stats

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

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

Examples

The following is sample output of the **show ip casa stats** command:

```
Router# show ip casa stats
Casa is active:
  Wildcard Stats:
    Wildcards:       6           Max Wildcards:    6
    Wildcard Denies: 0           Wildcard Drops:   0
    Pkts Throughput: 441         Bytes Throughput: 39120
  Affinity Stats:
    Affinities:      2           Max Affinities:   2
    Cache Hits:      444         Cache Misses:     0
    Affinity Drops:  0
  Casa Stats:
    Int Packet:      4           Int Tickle:       0
    Casa Denies:     0           Drop Count:       0
```

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

Table 7: show ip casa stats Field Descriptions

Field	Description
Casa is Active	The Forwarding Agent is active.
Wildcard Stats	Wildcard statistics.
Wildcards	Number of current wildcards.
Max Wildcards	Maximum number of wildcards since the Forwarding Agent became active.
Wildcard Denies	Protocol violations.
Wildcard Drops	Not enough memory to install wildcard.
Pkts Throughput	Number of packets passed through all wildcards.

Field	Description
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 8: show ip casa wildcard Field Descriptions

Field	Description
Source Address	Source address of a given TCP connection.
Source Mask	Mask to apply to source address before matching.
Port	Source port of a given TCP connection.
Dest Address	Destination address of a given TCP connection.
Dest Mask	Mask to apply to destination address before matching.
Port	Destination port of a given TCP connection.
Prot	Protocol of a given TCP connection.
Service Manager Details	Services manager details.
Manager Addr	Source address of this wildcard.
Insert Time	System time at which this wildcard was inserted.
Affinity Statistics	Affinity statistics.
Affinity Count	Number of affinities created on behalf of this wildcard.
Interest Packet Timeouts	Number of unanswered interest packets.
Packet Statistics	Packet statistics.
Packets	Number of packets that match this wildcard.
Bytes	Number of bytes that match this wildcard.
Action Details	Actions to be taken on a match.
Interest Addr	Services manager that is to receive interest packets for this wildcard.
Interest Port	Services manager port to which interest packets are sent.
Interest Packet	List of packet types that the services manager is interested in.

Field	Description
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 9: 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 10: 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 11: 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 12: show ip 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.

Field	Description
Remote port	Port number for the remote SCTP endpoint.
Primary dest addr	Primary destination address.
Effective primary dest addr	Current primary destination address.
Heartbeats	Status of heartbeats.
Timeout	Heartbeat timeout.
RTO/RTT/SRTT	Retransmission timeout, round trip time, and smoothed round trip time, calculated from network feedback.
TOS	IP precedence setting.
MTU	Maximum transmission unit size, in bytes, that a particular interface can handle.
cwnd	Congestion window value calculated from network feedback. This value is the maximum amount of data that can be outstanding in the network for that particular destination.
ssthresh	Slow-start threshold value calculated from network feedback.
outstand	Number of outstanding bytes.
Num retrans	Current number of times that data has been retransmitted to that address.
Max retrans	Maximum number of times that data has been retransmitted to that address.
Num times failed	Number of times that the address has been marked as failed.
Local vertag, Remote vertag	Verification tags (vertags). Tags are chosen during association initialization and do not change.
Num inbound streams, Num outbound streams	Maximum inbound and outbound streams. This number does not change.
Max assoc retrans	Maximum association retransmit limit. Number of times that any particular chunk may be retransmitted before a declaration that the association failed, which indicates that the chunk could not be delivered on any address.
Max init retrans	Maximum initial retransmit limit. Number of times that the chunks for initialization may be retransmitted before a declaration that the attempt to establish the association failed.
CumSack timeout	Cumulative selective acknowledge (SACK) timeout. The maximum time that a SACK may be delayed while attempting to bundle together with data chunks.

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

show ip sctp association statistics

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

To display statistics that have accumulated for the specified Stream Control Transmission Protocol (SCTP) association, use the **show ip sctp association statistics** command in privileged EXEC mode.

show ip sctp association statistics *assoc-id*

Syntax Description

assoc-id	Association identifier, which can be obtained from the output of the **show ip sctp association list** command.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp association statistics** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	Two new output fields were added to this command: Number of unordered data chunks sent and Number of unordered data chunks received. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(11)T	This command was replaced by the **show sctp association statistics** command.
12.4(15)T	This command was moved to the *Cisco IOS IP Application Services Command Reference*.

Usage Guidelines

This command shows only the information that has become available since the last time a **clear ip sctp statistics** command was executed.

Examples

The following sample output shows the statistics accumulated for SCTP association 0:

```
Router# show ip sctp association statistics 0

** SCTP Association Statistics **
AssocID/InstanceID: 0/1
Current State: ESTABLISHED
Control Chunks
  Sent: 623874  Rcvd: 660227
Data Chunks Sent
```

```
  Total: 14235644  Retransmitted: 60487
  Ordered: 6369678  Unordered: 6371263
  Avg bundled: 18  Total Bytes: 640603980
Data Chunks Rcvd
  Total: 14496585  Discarded: 1755575
  Ordered: 6369741  Unordered: 6371269
  Avg bundled: 18  Total Bytes: 652346325
  Out of Seq TSN: 3069353
ULP Dgrams
  Sent: 12740941  Ready: 12740961  Rcvd: 12740941
```

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

Table 13: show ip sctp association statistics Field Descriptions

Field	Description
AssocID/InstanceID	SCTP association identifier and instance identifier.
Current State	State of SCTP association.
Control Chunks	SCTP control chunks sent and received.
Data Chunks Sent	SCTP data chunks sent, ordered and unordered.
Data Chunks Rcvd	SCTP data chunks received, ordered and unordered.
ULP Dgrams	Number of datagrams sent, ready, and received by the Upper-Layer Protocol (ULP).

Related Commands

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

show ip sctp errors

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

To display the error counts logged by the Stream Control Transmission Protocol (SCTP), use the **show ip sctp errors** command in privileged EXEC mode.

show ip sctp errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp errors** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(11)T	This command was replaced by the **show sctp errors** command.
12.4(15)T	This command was moved to the *Cisco IOS IP Application Services Command Reference*.

Usage Guidelines

This command displays all errors across all associations that have been logged since the last time that the SCTP statistics were cleared with the **clear ip sctp statistics** command. If no errors have been logged, this is indicated in the output.

Examples

The following sample output shows a session with no errors:

```
Router# show ip sctp errors

*** SCTP Error Statistics ****
No SCTP errors logged.
```

The following sample output shows a session that has SCTP errors:

```
Router# show ip sctp errors

** SCTP Error Statistics **
Invalid verification tag:       5
```

```
Communication Lost:             64
Destination Address Failed:     3
Unknown INIT params rcvd:       16
Invalid cookie signature:       5
Expired cookie:                 1
Peer restarted:                 1
No Listening instance:          2
```

Field descriptions are self-explanatory.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
debug ip sctp api	Reports SCTP diagnostic information and messages.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.
show iua asp	Displays information about the current condition of an ASP.

show ip sctp instances

Note Effective with Cisco IOS Release 12.4(11)T, the **show ip sctp instances** command is replaced by the **show sctp instances** command. For more information, see the **show sctp instances** command.

To display information for each of the currently configured Stream Control Transmission Protocol (SCTP) instances, use the **show ip sctp instances** command in privileged EXEC mode.

show ip sctp instances

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp instances** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(11)T	This command was replaced by the **show sctp instances** command.
12.4(15)T	This command was moved to the *Cisco IOS IP Application Services Command Reference*.

Usage Guidelines

This command displays information for each of the currently configured instances. The instance number, local port, and address information are displayed. The instance state is either available or deletion pending. An instance enters the deletion pending state when a request is made to delete it but there are currently established associations for that instance. The instance cannot be deleted immediately and instead enters the pending state. No new associations are allowed in this instance, and when the last association is terminated or fails, the instance is deleted.

The default inbound and outbound stream numbers are used for establishing incoming associations, and the maximum number of associations allowed for this instance is shown. Then a snapshot of each existing association is shown, if any exists.

Effective with Cisco IOS Release 12.4(11)T, if you enter the **show ip sctp instances** command, you must type the complete word **instances** in the command syntax.

Examples

The following sample output shows available IP SCTP instances. In this example, two current instances are active and available. The first is using local port 8989, and the second is using 9191. Instance identifier 0 has three current associations, and instance identifier 1 has no current associations.

```
Router# show ip sctp instances

*** SCTP Instances ****
Instance ID:0  Local port:8989
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1
  Current associations: (max allowed:6)
  AssocID:0  State:ESTABLISHED  Remote port:8989
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:1  State:ESTABLISHED  Remote port:8990
    Dest addrs:10.6.0.4 10.5.0.4
  AssocID:2  State:ESTABLISHED  Remote port:8991
    Dest addrs:10.6.0.4 10.5.0.4
Instance ID:1  Local port:9191
Instance state:available
Local addrs:10.1.0.2 10.2.0.2
Default streams inbound:1  outbound:1
No current associations established for this instance.
Max allowed:6
```

Field descriptions are self-explanatory.

Related Commands

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

show ip sctp statistics

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

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

show ip sctp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)MB	This command was introduced as part of the **show ip sctp** command.
12.2(2)T	This command was changed to the **show ip sctp statistics** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.4(11)T	This command was replaced by the **show sctp statistics** command.
12.4(15)T	This command was moved to the *Cisco IP Application Services Command Reference*.

Usage Guidelines

This command displays the overall SCTP statistics accumulated since the last **clear ip sctp statistics** command. It includes numbers for all currently established associations, and for any that have been terminated. The statistics indicated are similar to those shown for individual associations.

Examples

The following sample output shows IP SCTP statistics:

```
Router# show ip sctp statistics

*** SCTP Overall Statistics ****
Total Chunks Sent:           2097
Total Chunks Rcvd:           2766
Data Chunks Rcvd In Seq:     538
Data Chunks Rcvd Out of Seq: 0
Total Data Chunks Sent:      538
Total Data Chunks Rcvd:      538
Total Data Bytes Sent:       53800
Total Data Bytes Rcvd:       53800
Total Data Chunks Discarded: 0
Total Data Chunks Retrans:   0
Total SCTP Dgrams Sent:      1561
Total SCTP Dgrams Rcvd:      2228
Total ULP Dgrams Sent:       538
Total ULP Dgrams Ready:      538
Total ULP Dgrams Rcvd:       538
```

Field descriptions are self-explanatory.

Related Commands

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