show tcp through start-forwarding agent

- show tcp, page 2
- show tcp brief, page 13
- show tcp statistics, page 15
- show tech-support, page 21
- show time-range ipc, page 30
- show track, page 32
- show track resolution, page 39
- show track route, page 41
- show udp, page 43
- show wccp, page 45
- show wccp global counters, page 52
- special-vj, page 54
- start-forwarding-agent, page 55

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 1: 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 2: 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 3: 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 4: 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 5: 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 6: 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 7: 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 8: 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 9: 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 10: 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.
Cisco IOS XE 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

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 11: 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.

Field	Description
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object.
First-hop interface is	Displays the first-hop interface.
Object type	Object type that is being tracked.
Poll Interval	Interval (in seconds) in which the tracking process polls the object.
Time to next poll	Period of time, in seconds, until the next polling of the object.

The following output shows that there are two objects. Object 1 has been configured with a weight of 10 “down,” and object 2 has been configured with a weight of 20 “up.” Object 1 is down (expressed as 0/10) and object 2 is up. The total weight of the tracked list is 20 with a maximum of 30 (expressed as 20/30). The “up” threshold is 20, so the list is “up.”

```
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 12: show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Boolean AND is Down	Each object defined in the list must be in a down state.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in *hh:mm:ss*) since the last change.
Tracked by	Client process that is tracking the object; in this case, HSRP.

The following example shows information about a stub object that has been created to be tracked using Embedded Event Manager (EEM):

```
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 13: 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.

Field	Description
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 14: 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 ip route	Tracks the state of an IP route and enters tracking configuration mode.

show track resolution

To display resolution information about objects that are tracked by a tracking process, use the **show track resolution** command in privileged EXEC mode.

show track resolution [**ip**| **ipv6**]

Syntax Description

ip	(Optional) Displays IP resolution parameters.
ipv6	(Optional) Displays IPv6 resolution parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(3)T	This command was modified. The valid range of the *object-number* argument increased to 1000.
15.1(1)S	This command was 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

Use this command to show the conversion factor applied to each routing protocol for IP or IPv6. If no parameter is specified, then the information for both IP and IPv6 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 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 resources. Testing should be conducted to ensure that the service works under specific site-traffic conditions.

Examples

The following example shows information about both IP and IPv6 route resolution:

```
Device# show track resolution

IP Route Resolution

Route type     Metric Resolution
static                 10
EIGRP            2560
OSPF                   1
ISIS                   10
BGP                    2560

IPv6 Route Resolution

Route type     Metric Resolution
static                 10
EIGRP            2560
OSPF                   1
ISIS                   10
BGP                    2560
```

The following example shows information about IPv6 route resolution:

```
Device# show track resolution IPv6

IPv6 Route Resolution

Route type     Metric Resolution
static                 10
EIGRP            2560
OSPF                   1
ISIS                   10
BGP              2560
```

Related Commands

Command	Description
showtrack	Displays information about objects that are tracked by a tracking process.
showtrack route	Displays tracked IP-route or IPv6-route objects.
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 track route

To display information about routes that are tracked by a tracking process, use the **show track route** command in privileged EXEC mode.

show track [**ip**| **ipv6**] **route [brief]**

Syntax Description

ip	(Optional) Displays information about tracked IP route parameters.
ipv6	(Optional) Displays information about tracked IPv6 route parameters.
brief	(Optional) Displays a summary for each tracked route, such as state and the time of the last state change.

Command Modes

Privileged EXEC (#)

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 modified. The **ipv6** keyword was added.

Usage Guidelines

Use this command to display information about IP or IPv6 routes that are tracked by a tracking process. If the **ip** or **ipv6** keywords are not specified, then information about both routes is displayed.

Examples

The following example shows brief information about IPv6 routes:

```
Device# show track ipv6 route brief
Track Type        Instance                  Parameter         State   Last Change
601   ipv6 route  2001:DB8:0:ABCD::1/48      metric threshold  Down    00:10:42
607   ipv6 route  2001:DB8:5:D::/64          metric threshold  up      00:05:10
608   ipv6 route  2001:DB8::1/64             metric threshold  up      00:06:08
```

```
612   ipv6 route  2001:DB8:0:1:FFFF::/64      reachability      Down    00:10:36
```

The following example shows information about IPv6 routes:

```
Device# show track ipv6 route
Track 607
  IPv6 route 2001::DB8::/64 metric threshold
  Metric threshold is Up (connected)
    5 change, last change 00:00:21
  Metric threshold down 255 up 254
  First-hop interface is Ethernet1/0
  Tracked by:
    HSRP Ethernet0/0 3
Track 608
  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 140 up 120
  First-hop interface is unknown
```

Related Commands

Command	Description
show track	Displays information about objects that are tracked by a tracking process.
show track route	Displays tracked IP-route or IPv6-route objects.
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 15: 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 16: 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 17: 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 18: 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 19: 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.