

1 TCP Commands

Command	Function
ip tcp keepalive	Enable the TCP keepalive function.
ip tcp mss	Configure the upper MSS limit for a TCP connection.
ip tcp path-mtu-discovery	Enable the path MTU discovery function of TCP.
ip tcp send-reset	Configure the sending of TCP reset packets upon the receiving of port unreachable messages.
ip tcp synwait-time	Configure the timeout period of SYN packets used for connection establishment.
ip tcp window-size	Configure the TCP window size.
show ipv6 tcp connect	Display the basic information about the current IPv6 TCP connection.
show ipv6 tcp connect statistics	Display the statistics on all the current IPv6 TCP connections.
show ipv6 tcp pmu	Display the path MTU of an IPv6 TCP connection.
show ipv6 tcp port	Display the usage of the current IPv6 TCP port.
show tcp connect	Display the basic information about the current IPv4 TCP connection.
show tcp connect statistics	Display the statistics on all the current IPv4 TCP connections.
show tcp parameter	Display the information about current TCP parameters.
show tcp pmu	Display the path MTU of an IPv4 TCP connection.
show tcp port	Display the usage of the current IPv4 TCP port.
show tcp statistics	Display the current TCP statistics of the system.

1.1 ip tcp keepalive

Function

Run the **ip tcp keepalive** command to enable the TCP keepalive function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The TCP keepalive function is disabled by default.

Syntax

```
ip tcp keepalive [ interval interval ] [ times times ] [ idle-period time ]
```

```
no ip tcp keepalive
```

```
default ip tcp keepalive
```

Parameter Description

interval *interval*: Indicates the interval time at which a keepalive packet is transmitted, in seconds. The value range is from 1 to 120. The default value is **75**.

times *times*: Indicates the keepalive packet transmission count. The value range is from 1 to 10, and the default value is **6**.

idle-period *time*: Indicates the idle period, in seconds, that is, the length of time that the peer end does not send a packet to the local end. The value range is from 60 to 1800. The default value is **900**, that is, 15 minutes.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

You may enable the keepalive function to check whether the peer end of a TCP connection works normally.

Suppose that the TCP keepalive function is enabled on a device and default interval, transmission count, and idle period settings are used. If no packet is received from the peer within 15 minutes, the device starts sending keepalive packets every 75 seconds for 6 consecutive times. If the device receives no TCP packet from the peer, it considers the TCP connection invalid and automatically releases the TCP connection.

This command is no different to the server and client and applies to all TCP connections.

Examples

The following example enables the TCP keepalive function on a device with the idle period, interval, and transmission count set to 3 minutes, 60 seconds, and 4 respectively.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

Notifications

N/A

Common Errors

N/A

Platform Description

This command has superseded the **service tcp-keepalives-in** and **service tcp-keepalives-out** commands.

Related Commands

N/A

1.2 ip tcp mss

Function

Run the **ip tcp mss** command to configure the upper MSS limit for a TCP connection.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

The calculated value "IPv4/IPv6 MTU – IPv4/IPv6 header length – TCP header length" is used as the upper MSS limit by default.

Syntax

ip tcp mss *max-segment-size*

no ip tcp mss

default ip tcp mss

Parameter Description

max-segment-size: Upper MSS limit. The value range is from 68 to 10000, in bytes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The MSS refers to the maximum length of data payload in a TCP segment, excluding the TCP option.

This command is used to restrict the MSS limit for TCP connections to be established. The negotiated MSS for a new connection should be smaller than this MSS.

This parameter does not need to be configured by default. Instead, the MSS calculated based on the MTU is used, as shown below:

IPv4 TCP: MSS = IP MTU of the outbound interface corresponding to the peer IP address – IP header size (20 bytes) – TCP header size (20 bytes).

IPv6 TCP: MSS = Path MTU corresponding to the peer IPv6 address – IPv6 header size (40 bytes) – TCP header size (20 bytes).

If a connection supports certain options, the option length after 4-byte alignment should be deducted from the MSS value. For example, 20 bytes need to be deducted if the MD5 option is used because the length of the MD5 option is 18 bytes and the length after alignment is 20 bytes.

If an upper MSS limit is configured, the upper MSS limit that actually takes effect is the MSS calculated based on the MTU or configured MSS, whichever is smaller.

Examples

The following example sets the upper MSS limit of TCP connections to 1,300 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp mss 1300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip tcp path-mtu-discovery

Function

Run the **ip tcp path-mtu-discovery** command to enable the path MTU discovery function of TCP.

Run the **no** form of this command to disable this feature.

The path MTU discovery function of TCP is disabled by default.

Syntax

```
ip tcp path-mtu-discovery [ age-timer time | age-timer infinite ]
```

```
no ip tcp path-mtu-discovery
```

Parameter Description

age-timer *time*: Indicates the interval for a new probe after TCP discovers a path MTU, in minutes. The value range is from 10 to 30. The default value is **10**.

age-timer infinite: Indicates that no probe is performed after TCP discovers a path MTU.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The path MTU discovery function of TCP is implemented according to RFC1191 to improve the network bandwidth utilization. When TCP is applied to bulk transmit chunk data, this function can improve transmission performance greatly.

After discovering the path MTU, TCP can use a larger MSS to probe a new path MTU at intervals. This interval is specified by using the **age-timer** parameter. When the device discovers a path MTU smaller than the MSS negotiated by both ends of a TCP connection, the device tries to probe a larger path MTU at the configured interval described above. The probe process is stopped when the path MTU reaches the MSS or the user turns off the timer. You may use the **age-timer infinite** parameter to turn off this timer.

This command applies to only IPv4 TCP. The path MTU discovery function of IPv6 TCP is enabled permanently and cannot be disabled.

Examples

The following example enables the path MTU discovery function of TCP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp path-mtu-discovery
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip tcp send-reset

Function

Run the **ip tcp send-reset** command to configure the sending of TCP reset packets upon the receiving of port unreachable messages.

Run the **no** form of this command to remove this configuration.

TCP reset packets are sent upon the receiving of port unreachable messages by default.

Syntax

ip tcp send-reset

no ip tcp send-reset

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In general, when the TCP module distributes a TCP packet, if the TCP connection, to which the packet belongs, cannot be identified, the local end sends a reset packet to the peer end to terminate the TCP connection. This, however, can also become a target for attackers. A large number of TCP port unreachable messages can impose attacks on the device. You can use this command to prevent the sending of TCP reset packets upon the receiving of port unreachable messages.

This command applies to both IPv4 TCP and IPv6 TCP.

Examples

The following example configures the device not to send TCP reset packets upon the receiving of port unreachable messages.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip tcp send-reset
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip tcp synwait-time

Function

Run the **ip tcp synwait-time** command to configure the timeout period of SYN packets used for connection establishment.

Run the **no** form of this command to restore the default configuration.

The default timeout period of SYN packets used for connection establishment is 20 seconds.

Syntax

ip tcp synwait-time *time*

no ip tcp synwait-time

Parameter Description

time: SYN packet timeout period, in seconds. The value range is from 5 to 300. The default value is **20**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In case of SYN flooding, shortening SYN timeout period can reduce resource consumption. However, it does not work on continuous SYN flooding.

When a device actively requests to establish a connection with an external device, shortening SYN timeout period can reduce users' waiting time, for example, waiting time in the telnet connection. You may prolong SYN timeout period properly for a poor network.

This command applies to both IPv4 TCP and IPv6 TCP.

Examples

The following example sets the timeout period of SYN packets used for connection establishment to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp synwait-time 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 ip tcp window-size

Function

Run the **ip tcp window-size** command to configure the TCP window size.

Run the **no** form of this command to restore the default configuration.

The default TCP window size is 65,535 bytes.

Syntax

ip tcp window-size *size*

no ip tcp window-size

Parameter Description

size: Window size, in bytes. The value range is from 128 to 1073725440.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The TCP receive buffer is used to buffer data from the peer. The data will be subsequently read by applications. The TCP window size reflects the size of idle space in the receive buffer. For bulk-data connections, enlarging the window size dramatically promotes TCP transmission performance.

If the window size is greater than 65535 bytes, window enlarging will be enabled automatically.

This command applies to both IPv4 TCP and IPv6 TCP.

Examples

The following example sets the TCP window size to 16,386 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tcp window-size 16386
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 show ipv6 tcp connect

Function

Run the **show ipv6 tcp connect** command to display the basic information about the current IPv6 TCP connection.

Syntax

```
show ipv6 tcp connect [ local-ipv6 ipv6-address ] [ local-port port-number ] [ peer-ipv6 ipv6-address ] [ peer-port port-number ] [ vrf-name vrf-name ]
```

Parameter Description

local-ipv6 *ipv6-address*: Indicates a local IPv6 address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ipv6 *ipv6-address*: Indicates a peer IPv6 address. The value range is from 1 to 65535.

peer-port *port-number*: Indicates a peer port.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the basic information about all IPv6 TCP connections is displayed.

Examples

The following example displays the basic information about the current IPv6 TCP connections.

```
Hostname> enable
Hostname# show ipv6 tcp connect
Number Local Address      Foreign Address          State      Process name
1      :::22                   :::0                     LISTEN    orion-sshd
2      :::23                   :::0                     LISTEN    orion-telnetd
3      1000::1:23             1000::2:64201           ESTABLISHED orion-telnetd
```

The following example displays the basic information about the current IPv6 TCP connection in VRF-IPv6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# vrf definition vrf-ipv6
Hostname(config-vrf)# address-family ipv6
Hostname(config-vrf-af)# show ipv6 tcp connect vrf-name vrf-ipv6
Number  Local Address  Foreign Address          STATE      Process name
VRF name
1      :::23          :::0                     LISTEN    telnetd-main
vrf-ipv6
```

Table 1-1 Output Fields of the show ipv6 tcp connect Command

Field	Description
Number	Serial number.

Field	Description
Local Address	Local address and port number. The number after the last colon is the port number.
Foreign Address	Remote address and port number. The number after the last colon is the port number.
State	<p>Current status of a TCP connection:</p> <ul style="list-style-type: none"> ● CLOSED: Indicates that the connection is closed. ● LISTEN: Indicates the listening status. ● SYNSENT: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● SYNRCVD: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● ESTABLISHED: Indicates that the connection is established. ● FINWAIT1: Indicates that the FIN packet has been sent from the local end. ● FINWAIT2: Indicates that the FIN packet sent from the local end has been acknowledged. ● CLOSEWAIT: Indicates that the local end has received the FIN packet from the peer end. ● LASTACK: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● CLOSING: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● TIMEWAIT: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● NEW_SYN_RECV: Indicates a new TCP connection request.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.8 show ipv6 tcp connect statistics

Function

Run the **show ipv6 tcp connect statistics** command to display the statistics on all the current IPv6 TCP connections.

Syntax

```
show ipv6 tcp connect statistics
```

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the statistics on all the current IPv6 TCP connections.

```
Hostname# show ipv6 tcp connect statistics

State          Count
-----
ESTABLISHED    1
SYN_SENT       0
SYN_RECV       0
FIN_WAIT1      0
FIN_WAIT2      0
TIME_WAIT      0
CLOSED         0
CLOSE_WAIT     0
LAST_ACK       0
LISTEN         15
CLOSING        0
NEW_SYN_RECV   0
Total: 16
```

Table 1-1 Output Fields of the show ipv6 tcp connect statistics Command

Field	Description
State	<p>Current status of a TCP connection:</p> <ul style="list-style-type: none"> ● CLOSED: Indicates that the connection is closed. ● LISTEN: Indicates the listening status. ● SYNSENT: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● SYNRCVD: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● ESTABLISHED: Indicates that the connection is established. ● FINWAIT1: Indicates that the FIN packet has been sent from the local end. ● FINWAIT2: Indicates that the FIN packet sent from the local end has been acknowledged. ● CLOSEWAIT: Indicates that the local end has received the FIN packet from the peer end. ● LASTACK: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● CLOSING: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● TIMEWAIT: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● NEW_SYN_RECV: Indicates a new TCP connection request.
Count	Number of times that connections are in a specific state.
Total	Total count.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.9 show ipv6 tcp pmtu**Function**

Run the **show ipv6 tcp pmtu** command to display the path MTU of an IPv6 TCP connection.

Syntax

```
show ipv6 tcp pmtu [ local-ipv6 ipv6-address ] [ local-port port-number ] [ peer-ipv6 ipv6-address ] [ peer-port port-number ] [ vrf-name vrf-name ]
```

Parameter Description

local-ipv6 *ipv6-address*: Indicates a local IPv6 address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ipv6 *ipv6-address*: Indicates a peer IPv6 address.

peer-port *port-number*: Indicates a peer port. The value range is from 1 to 65535.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the path MTUs of all IPv6 TCP connections are displayed.

Examples

The following example displays the path MTUs of IPv6 TCP connections.

```

Hostname> enable
Hostname# show ipv6 tcp pmtu
Number  Local Address          Foreign Address          PMTU
1       1000::1:23              1000::2.13560           1440

```

Table 1-1 Output Fields of the `show ipv6 tcp pmtu` Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the last colon is the port number.
Foreign Address	Remote address and port number. The number after the last colon is the port number.
PMTU	Path MTU.

Notifications

N/A

Platform Description

N/A

Related Commands

- `show vrf` (IP routing/VRF)

1.10 show ipv6 tcp port

Function

Run the **show ipv6 tcp port** command to display the usage of the current IPv6 TCP port.

Syntax

```
show ipv6 tcp port [ port-number ]
```

Parameter Description

port-number: Specified port number. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the usage of all current IPv6 TCP ports is displayed.

Examples

The following example displays the usage of the current IPv6 TCP ports.

```

Hostname> enable
Hostname# show ipv6 tcp port
TCP connections on port 23:
Number  Local Address Foreign Address  State
1       1000::1:23    1000::2:64571  ESTABLISHED
Total: 1
TCP connections on port 2650:
Number  Local Address Foreign Address  State
Total: 0

```

Table 1-1 Output Fields of the show ipv6 tcp port Command

Field	Description
Number	Serial number.
Local Address	Local address and port number.
Foreign Address	Remote address and port number.

Field	Description
State	<p>Current status of a TCP connection:</p> <ul style="list-style-type: none"> ● CLOSED: Indicates that the connection is closed. ● LISTEN: Indicates the listening status. ● SYNSENT: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● SYNRCVD: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● ESTABLISHED: Indicates that the connection is established. ● FINWAIT1: Indicates that the FIN packet has been sent from the local end. ● FINWAIT2: Indicates that the FIN packet sent from the local end has been acknowledged. ● CLOSEWAIT: Indicates that the local end has received the FIN packet from the peer end. ● LASTACK: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● CLOSING: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● TIMEWAIT: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● NEW_SYN_RECV: Indicates a new TCP connection request.
Total	Total number of information entries.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show tcp connect

Function

Run the **show tcp connect** command to display the basic information about the current IPv4 TCP connection.

Syntax

```
show tcp connect [ local-ip ip-address ] [ local-port port-number ] [ peer-ip ip-address ] [ peer-port port-number ] [ vrf-name vrf-name ]
```

Parameter Description

local-ip ip-address: Indicates a local IP address.

local-port port-number: Indicates a local port. The value range is from 1 to 65535.

peer-ip *ip-address*: Indicates a peer IP address.

peer-port *port-number*: Indicates a peer port. The value range is from 1 to 65535.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is not configured, the basic information about all IPv4 TCP connections is displayed.

Examples

The following example displays the basic information about the current IPv4 TCP connections.

```

Hostname> enable
Hostname# show tcp connect
Number Local Address      Foreign Address          State      Process name
1      0.0.0.0:22              0.0.0.0:0                LISTEN    orion-sshd
2      0.0.0.0:23              0.0.0.0:0                LISTEN    orion-telnetd
3      1.1.1.1:23              1.1.1.2:64201            ESTABLISHED orion-telnetd

```

Table 1-1Output Fields of the show tcp connect Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the colon is the port number, for example, "23" in "1.1.1.1:23" is a port number.
Foreign Address	Remote address and port number. The number after the colon is the port number, for example, "23" in "1.1.1.1:23" is a port number.

Field	Description
State	<p>Current status of a TCP connection:</p> <ul style="list-style-type: none"> ● CLOSED: Indicates that the connection is closed. ● LISTEN: Indicates the listening status. ● SYNSENT: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● SYNRCVD: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● ESTABLISHED: Indicates that the connection is established. ● FINWAIT1: Indicates that the FIN packet has been sent from the local end. ● FINWAIT2: Indicates that the FIN packet sent from the local end has been acknowledged. ● CLOSEWAIT: Indicates that the local end has received the FIN packet from the peer end. ● LASTACK: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● CLOSING: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● TIMEWAIT: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● NEW_SYN_RECV: Indicates a new TCP connection request.
Process name	Process name.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.12 show tcp connect statistics

Function

Run the **show tcp connect statistics** command to display the statistics on all the current IPv4 TCP connections.

Syntax

show tcp connect statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the statistics on all the current IPv4 TCP connection.

```
Hostname> enable
Hostname# show tcp connect statistics
State                Count
-----
ESTABLISHED          23
SYN_SENT              36
SYN_RECV              0
FIN_WAIT1             0
FIN_WAIT2             0
TIME_WAIT             0
CLOSED                0
CLOSE_WAIT           0
LAST_ACK              0
LISTEN                23
CLOSING               0
NEW_SYN_RECV          0
Total: 82
```

Table 1-1 Output Fields of the show tcp connect statistics Command

Field	Description
State	<p>Current status of a TCP connection:</p> <ul style="list-style-type: none"> ● CLOSED: Indicates that the connection is closed. ● LISTEN: Indicates the listening status. ● SYNSENT: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● SYNRCVD: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● ESTABLISHED: Indicates that the connection is established. ● FINWAIT1: Indicates that the FIN packet has been sent from the local end. ● FINWAIT2: Indicates that the FIN packet sent from the local end has been acknowledged. ● CLOSEWAIT: Indicates that the local end has received the FIN packet from the peer end. ● LASTACK: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● CLOSING: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● TIMEWAIT: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● NEW_SYN_RECV: Indicates a new TCP connection request.
Count	Number of times that connections are in a specific state.
Total	Total count.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show tcp parameter**Function**

Run the **show tcp parameter** command to display the information about current TCP parameters.

Syntax

```
show tcp parameter
```

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example displays the information about the current TCP parameters.

```
Hostname> enable
Hostname# show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)
  Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit:
bytes)
  Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit: bytes)
  Current allocated memory: 0
  Current memory pressure flag: 0
SYN specific information:
  Max SYN_RECV sockets per LISTEN socket: 65535
  Max SYN retries: 5
  Max SYN ACK retries: 5
Timewait specific information:
  Max timewait sockets: 180000
  Current timewait sockets: 0
  Timewait recycle: 0
  Reuse timewait port: 0
Keepalive information:
  Keepalive on: 0
  Idle period: 900 seconds
  Interval: 75 seconds
  Max probes: 6
MTU probing:
  Enable mtu probing: 0
FIN specific information:
  FIN_WAIT_2 timeout: 60 seconds
Orphan socket information:
  Max orphans: 16384
```

```
Max orphan retries: 0
Current orphans: 0
```

Table 1-1 Output Fields of the show tcp parameter Command

Field	Description
Hash table information	Hash table information of TCP connections.
Established hash bucket size	Hash bucket size of TCP connections in established status.
Bind hash bucket size	Hash bucket size of a listening port.
Memory information	Parameter information of Rx and Tx buffers of TCP connections.
Global memory limit	Global memory limit.
low=x	Memory limit of TCP sockets.
pressure=x	Memory alarm level of TCP sockets.
high=x (unit: pages)	Maximum memory usage of TCP sockets. The system will deny allocating sockets when the memory usage exceeds this value.
Per-socket receive buffer size	Size of the socket Rx buffer.
min=x	Minimum size of the socket buffer.
default=x	Default size of the socket buffer.
max=x (unit: bytes)	Maximum size of the socket buffer.
Per-socket send buffer size	Size of the socket Tx buffer.
Current allocated memory	Memory currently used by sockets.
Current memory pressure flag	Whether the current memory usage of sockets exceeds the alarm level.
SYN specific information	Parameter information related to connections and listening on the TCP server side.
Max SYN_RECV sockets per LISTEN socket	Maximum number of SYN connections of the listening socket.
Max SYN retries	Maximum retransmission count of SYN packets.
Max SYN ACK retries	Maximum retransmission count of SYN ACK packets.
Timewait specific information	Parameter information of TCP connections in TIME-WAIT status.
Max timewait sockets	Maximum number of TCP connections in TIME-WAIT status.
Current timewait sockets	Number of current TCP connections in TIME-WAIT status.
Timewait recycle	Quick reclamation of TCP connections in TIME-WAIT status.
Reuse timewait port	Port reuse of TCP connections in TIME-WAIT status.

Field	Description
Keepalive information	Parameter information of the TCP keepalive time.
Keepalive on	Whether the TCP keepalive function is enabled.
Idle period	Idle period of TCP keepalive.
Interval	TCP keepalive interval.
Max probes	TCP keepalive probing count.
MTU probing	Parameter information related to MTU probing.
Enable mtu probing	Whether MTU probing is enabled.
FIN specific information	Parameter information related to closing of TCP connections.
FIN_WAIT_2 timeout	Timeout period in FIN-WAIT-2 status.
Orphan socket information	Parameter information of TCP connections not associated with a specific application.
Max orphans	Maximum number of TCP connections not associated with a specific application.
Max orphan retries	Maximum retransmission count of TCP packets not associated with a specific application.
Current orphans	Number of current TCP connections not associated with a specific application.

Notifications

N/A

1.14 show tcp pmtu

Function

Run the **show tcp pmtu** command to display the path MTU of an IPv4 TCP connection.

Syntax

```
show tcp pmtu [ local-ip ip-address ] [ local-port port-number ] [ peer-ip ip-address ] [ peer-port port-number ] [ vrf-name vrf-name ]
```

Parameter Description

local-ip *ip-address*: Indicates a local IP address.

local-port *port-number*: Indicates a local port. The value range is from 1 to 65535.

peer-ip *ip-address*: Indicates a peer IP address.

peer-port *port-number*: Indicates a peer port. The value range is from 1 to 65535.

vrf-name *vrf-name*: Specifies a VRF instance. The value is a VRF instance existing on the device.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the path MTUs of all IPv4 TCP connections are displayed.

Examples

The following example displays the path MTUs of IPv4 TCP connections.

```

Hostname> enable
Hostname# show tcp pmtu
Number  Local Address           Foreign Address          PMTU
1       192.168.195.212.23      192.168.195.112.13560  1440

```

Table 1-1 Output Fields of the show tcp pmtu Command

Field	Description
Number	Serial number.
Local Address	Local address and port number. The number after the colon is the port number, for example, "23" in "192.168.195.212.23" is a port number.
Foreign Address	Remote address and port number. The number after the colon is the port number, for example, "23" in "192.168.195.212.23" is a port number.
PMTU	Path MTU.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show vrf** (IP routing/VRF)

1.15 show tcp port

Function

Run the **show tcp port** command to display the usage of the current IPv4 TCP port.

Syntax

show tcp port [*port-number*]

Parameter Description

port-number: Specified port number. The value range is from 1 to 65535.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

If no parameter is configured, the usage of all current IPv4 TCP ports is displayed.

Examples

The following example displays the usage of the current IPv4 TCP ports.

```

Hostname> enable
Hostname#show tcp port
TCP connections on port 23:
Number  Local Address Foreign Address   State
1       1.1.1.1:23    1.1.1.2:64571    ESTABLISHED
Total: 1
TCP connections on port 2650:
Number  Local Address Foreign Address   State
Total: 0

```

Table 1-1 Output Fields of the show tcp port Command

Field	Description
Number	Serial number.
Local Address	Local address and port number.
Foreign Address	Remote address and port number.

State	<p>Current status of a TCP connection:</p> <ul style="list-style-type: none"> ● CLOSED: Indicates that the connection is closed. ● LISTEN: Indicates the listening status. ● SYNSENT: Indicates that the SYN packet is sent, and the connection is in the three-way handshake process. ● SYNRCVD: Indicates that the SYN packet is received, and the connection is in the three-way handshake process. ● ESTABLISHED: Indicates that the connection is established. ● FINWAIT1: Indicates that the FIN packet has been sent from the local end. ● FINWAIT2: Indicates that the FIN packet sent from the local end has been acknowledged. ● CLOSEWAIT: Indicates that the local end has received the FIN packet from the peer end. ● LASTACK: Indicates that the local end has received the FIN packet from the peer end and the local end has sent its own FIN packet. ● CLOSING: Indicates that the local end has sent the FIN packet, it has not received the ACK packet, but receives the FIN packet from the peer end. ● TIMEWAIT: Indicates that the FIN packet from the local end is acknowledged, and the local end has acknowledged the received FIN packet. ● NEW_SYN_RECV: Indicates a new TCP connection request.
Total	Total number of information entries.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.16 show tcp statistics

Function

Run the **show tcp statistics** command to display the current TCP statistics of the system.

Syntax

show tcp statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display the current TCP statistics of the system, including packet receiving information, three-way handshake information, and time-wait connection information.

Examples

The following example displays the current TCP statistics of the system.

```

Hostname> enable
Hostname#show tcp statistics
TCP Packets
  Received: 23243
  Errors   : 0(checksum: 0)
Three way handshake
  Request queue overflow: 0
  Accept backlog full: 0
  Web authentication limit per user: 0
  Failed to alloc memory for request sock: 0
  Failed to create open request child: 0
  SYN ACK retransmits: 0
  Timeouted requests: 0
  Web authentication:
    Limit per user: 0
    SYN ACK retransmission times-users: 0-0,1-0, 2-0,>=3-0
    Handshake fails: 0
Time-wait
  Time-wait bucket table overflow: 0

```

Table 1-1 Output Fields of the show tcp statistics Command

Field	Description
TCP Packets	Statistics on TCP packets received.
Received	Number of TCP packets received.
Errors	Number of TCP error packets received.
Three way handshake	Information about the three-way handshake process.
Request queue overflow	Number of packets discarded due to SYN queue overflow.
Accept backlog full	Number of packets discarded due to Accept queue overflow
Web authentication limit per user	Maximum concurrency of three-way handshake processes supported by a terminal to complete Web-based authentication.
Failed to alloc memory for request sock	Number of memory request failures in the three-way handshake process.

Failed to create open request child	Number of failures to enable subnodes in the three-way handshake process.
SYN ACK retransmits	SYN ACK packet retransmission count.
Timeouted requests	Timeout in the three-way handshake process.
Time-wait	Information about the connection in TIME-WAIT status.
Time-wait bucket table overflow	Overflow statistics of connections in TIME-WAIT status.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A