

目 录

1 IP性能优化.....	1-1
1.1 IP性能优化配置命令.....	1-1
1.1.1 display icmp statistics	1-1
1.1.2 display ip statistics	1-2
1.1.3 display rawip.....	1-4
1.1.4 display rawip verbose	1-5
1.1.5 display tcp.....	1-8
1.1.6 display tcp statistics	1-10
1.1.7 display tcp verbose	1-14
1.1.8 display udp.....	1-18
1.1.9 display udp statistics	1-19
1.1.10 display udp verbose.....	1-20
1.1.11 ip forward-broadcast.....	1-23
1.1.12 ip icmp error-interval.....	1-24
1.1.13 ip icmp fragment discarding.....	1-25
1.1.14 ip icmp source	1-26
1.1.15 ip mtu	1-26
1.1.16 ip redirects enable.....	1-27
1.1.17 ip ttl-expires enable	1-28
1.1.18 ip unreachable enable	1-29
1.1.19 reset ip statistics	1-29
1.1.20 reset tcp statistics	1-30
1.1.21 reset udp statistics	1-30
1.1.22 tcp mss.....	1-31
1.1.23 tcp path-mtu-discovery.....	1-32
1.1.24 tcp syn-cookie enable	1-32
1.1.25 tcp timer fin-timeout.....	1-33
1.1.26 tcp timer syn-timeout	1-34
1.1.27 tcp window	1-34

1 IP性能优化



说明

IP性能优化功能中所指的“接口”为三层接口，包括VLAN接口、三层以太网接口等。三层以太网接口是指在以太网接口视图下通过 **port link-mode route** 命令切换为三层模式的以太网接口，有关以太网接口模式切换的操作，请参见“二层技术-以太网交换配置指导”中的“以太网接口配置”。

1.1 IP性能优化配置命令

1.1.1 display icmp statistics

display icmp statistics 命令用来显示 ICMP 流量统计信息。

【命令】

display icmp statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 ICMP 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display icmp statistics 命令用来显示设备接收和发送的各类 ICMP 流量的统计信息。

【举例】

显示 ICMP 流量统计信息。

```
<Sysname> display icmp statistics
  Input: bad formats      0                bad checksum          0
         echo             175            destination unreachable 0
         source quench   0                redirects             0
         echo replies    201            parameter problem     0
         timestamp       0                information requests  0
         mask requests   0                mask replies          0
         time exceeded   0                invalid type          0
         router advert   0                router solicit        0
         broadcast/multicast echo requests ignored 0
```

```

broadcast/multicast timestamp requests ignored      0
Output: echo          0                            destination unreachable 0
        source quench 0                            redirects              0
        echo replies  175                          parameter problem     0
        timestamp     0                            information replies   0
        mask requests 0                            mask replies          0
        time exceeded 0                            bad address           0
        packet error  1442                          router advert         3

```

表1-1 display icmp statistics 命令显示信息描述表

字段	描述
bad formats	输入的格式错误报文数
bad checksum	输入的校验和错误报文数
echo	输入/输出的响应请求报文数
destination unreachable	输入/输出的目的不可达报文数
source quench	输入/输出的源站抑制报文数
redirects	输入/输出的重定向报文数
echo replies	输入/输出的响应应答报文数
parameter problem	输入/输出的参数错误报文数
timestamp	输入/输出的时间戳报文数
information requests	输入的信息请求报文数
mask requests	输入/输出的掩码请求报文数
mask replies	输入/输出的掩码应答报文数
invalid type	输入的非类型报文数
router advert	输入的路由器公告报文数
router solicit	输入的路由器请求报文数
broadcast/multicast echo requests ignored	输入的广播/组播响应请求丢弃报文数
broadcast/multicast timestamp requests ignored	输入的广播/组播时戳请求丢弃报文数
information replies	输出的信息应答报文数
time exceeded	输入/输出的超时报文数
bad address	输出的目的地址非法报文数
packet error	输出的错误报文数
router advert	输入/输出的路由器公告报文数

1.1.2 display ip statistics

display ip statistics 命令用来显示 IP 报文统计信息。

【命令】

display ip statistics [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 IP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display ip statistics 命令用来显示 IP 报文统计信息，包括接收报文、发送报文、分片、重组的统计信息。

【举例】

显示 IP 报文统计信息。

```
<Sysname> display ip statistics
  Input:  sum          7120          local          112
         bad protocol  0           bad format     0
         bad checksum  0           bad options    0
  Output: forwarding   0           local          27
         dropped       0           no route       2
         compress fails 0
  Fragment:input      0           output         0
         dropped       0
         fragmented    0           couldn't fragment 0
  Reassembling:sum    0           timeouts       0
```

表1-2 display ip statistics 命令显示信息描述表

	字段	描述
Input:	sum	接收报文总数
	local	接收的目的地址是本地的报文数
	bad protocol	未知协议的报文数
	bad format	格式错误的报文数
	bad checksum	校验和错误的报文数
	bad options	选项错误的报文数

	字段	描述
Output:	forwarding	转发的报文数
	local	本地发送报文数
	dropped	发送时丢弃的报文数
	no route	查不到路由的报文数
	compress fails	压缩失败的报文数
Fragment:	input	接收的分片报文数
	output	发送的分片报文数
	dropped	丢弃的分片报文数
	fragmented	分片成功的报文数
	couldn't fragment	分片失败的报文数
Reassembling:	sum	重组的报文总数
	timeouts	重组超时的分片报文数

【相关命令】

- **display ip interface**（三层技术-IP 业务命令参考/IP 地址）
- **reset ip statistics**

1.1.3 display rawip

display rawip 命令用来显示 RawIP 连接摘要信息。

【命令】

display rawip [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的 RawIP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display rawip 命令用来显示 RawIP 连接摘要信息，包括本端 IP 地址、对端 IP 地址、使用 RawIP socket 的协议号等信息。

【举例】

显示 RawIP 连接摘要信息。

```

<Sysname> display rawip
Local Addr      Foreign Addr    Protocol  Slot  PCB
0.0.0.0        0.0.0.0        1         1     0x0000000000000009
0.0.0.0        0.0.0.0        1         1     0x0000000000000008
0.0.0.0        0.0.0.0        1         1     0x0000000000000002

```

表1-3 display rawip 命令显示信息描述表

字段	描述
Local Addr	本端IP地址
Foreign Addr	对端IP地址
Protocol	使用RawIP socket的协议号
Slot	设备在IRF中的成员编号
PCB	协议控制块索引

1.1.4 display rawip verbose

display rawip verbose 命令用来显示 RawIP 连接详细信息。

【命令】

```
display rawip verbose [ slot slot-number [ pcb pcb-index ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

pcb pcb-index: 显示指定协议控制块索引的 RawIP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 RawIP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display rawip verbose 命令用来显示 RawIP 连接详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号等，以及 RawIP 连接的源 IP 地址和目的 IP 地址等信息。

【举例】

显示 RawIP 连接详细信息。

```

<Sysname> display rawip verbose
Total RawIP socket number: 1
Slot: 6
Creator: ping[320]
State: N/A

```

```

Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 9216 / 1 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 3
Protocol: 1
Connection info: src = 0.0.0.0, dst = 0.0.0.0
Inpcb flags: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff

```

表1-4 display rawip verbose 命令显示信息描述表

字段	描述
Total RawIP socket number	RawIP socket总数
Slot	设备在IRF中的成员编号
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： <ul style="list-style-type: none"> • NOFDREF: 用户已经关闭 • ISCONNECTED: 连接已经建立 • ISCONNECTING: 正在建立连接 • ISDISCONNECTING: 正在断开连接 • ASYNC: 异步方式 • ISDISCONNECTED: 连接已经断开 • PROTOREF: 协议强关联 • N/A: 不处于上述状态

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> SO_DEBUG: 记录套接字的调试信息 SO_ACCEPTCONN: server 端监听连接请求 SO_REUSEADDR: 允许本地地址重复使用 SO_KEEPALIVE: 协议需要查询空闲的连接 SO_DONTROUTE: 设置不查路由表（用于目的地址是直连网络的情况） SO_BROADCAST: 套接字支持广播报文 SO_LINGER: 套接字关闭但仍发送剩余数据 SO_OOBINLINE: 带外数据采用内联方式存储 SO_REUSEPORT: 允许本地端口重复使用 SO_TIMESTAMP: 记录入报文时间戳，只对非连接的协议有效，时间精确到毫秒 SO_NOSIGPIPE: socket 不能发送数据导致返回失败时不创建 SIGPIPE SO_FILTER: 设置报文过滤条件，对接收报文有效 SO_TIMESTAMPNS: 和时间戳选项功能类似，时间可以精确到纳秒 N/A: 没有设置选项
Error	影响socket连接的错误码
Receiving buffer (cc/hiwat/lowat/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> CANTSENDMORE: 不能发送数据到对端 CANTRCVMORE: 不能从对端接收数据 RCVATMARK: 接收标记 N/A: 不处于上述状态
Sending buffer (cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> CANTSENDMORE: 不能发送数据到对端 CANTRCVMORE: 不能从对端接收数据 RCVATMARK: 接收标记 N/A: 不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> 1: SOCK_STREAM, 流模式，提供可靠的字节流。TCP 协议使用此类型 2: SOCK_DGRAM, 数据报模式的通信。UDP 协议使用此类型 3: SOCK_RAW, RAW 模式的通信方式 N/A: 不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址、目的IP地址

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • (暂不支持) INP_SNDBYLSPV: 通过 MPLS 发送 • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_USEICMPSRC: 使用配置的 ICMP 地址作为源地址 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL(minimum TTL)	Internet协议控制块中的生存周期，括号中为最小生存周期
Send VRF	(暂不支持) 发送实例
Receive VRF	(暂不支持) 接收实例

1.1.5 display tcp

display tcp 命令用来显示 TCP 连接摘要信息。

【命令】

display tcp [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 TCP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display tcp 命令用来显示 TCP 连接摘要信息，包括本端 IP 地址及端口号、对端 IP 地址及端口号、TCP 连接的状态等信息。

【举例】

显示 TCP 连接摘要信息。

```
<Sysname> display tcp
*: TCP MD5 Connection
Local Addr:port      Foreign Addr:port    State      Slot PCB
*0.0.0.0:21          0.0.0.0:0           LISTEN     1      0x0000000000000c387
192.168.20.200:23    192.168.20.14:1284 ESTABLISHED 1      0x0000000000000009
192.168.20.200:23    192.168.20.14:1283 ESTABLISHED 1      0x0000000000000002
```

表1-5 display tcp 命令显示信息描述表

字段	描述
*	如果某个连接前有此标识，则表示该TCP连接是采用MD5加密算法认证的连接
Local Addr:port	本端IP地址及端口号
Foreign Addr:port	对端IP地址及端口号
State	TCP连接状态，可能的状态如下： <ul style="list-style-type: none">• CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态• LISTEN：服务器在等待连接请求时所处的状态• SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态• SYN_RCVD：服务器收到客户端连接请求时所处的状态• ESTABLISHED：服务器和客户端双方建立连接并能进行双向数据传递的状态• CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态• FIN_WAIT_1：客户端发出关闭连接请求等待服务器回应时所处的状态• CLOSING：连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态• LAST_ACK：服务器向客户端发出关闭连接请求等待回应时所处的状态• FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态• TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态
Slot	设备在IRF中的成员编号

字段	描述
PCB	协议控制块索引

1.1.6 display tcp statistics

display tcp statistics 命令用来显示 TCP 连接的流量统计信息。

【命令】

display tcp statistics [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的 TCP 连接流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display tcp statistics 命令用来显示 TCP 连接的流量统计信息，包括接收报文、发送报文以及 Syncookie/syncookie 等相关统计信息。

【举例】

显示 TCP 连接的流量统计信息。

```
<Sysname> display tcp statistics
Received packets:
  Total: 4150
  packets in sequence: 1366 (134675 bytes)
  window probe packets: 0, window update packets: 0
  checksum error: 0, offset error: 0, short error: 0
  packets dropped for lack of memory: 0
  packets dropped due to PAWS: 0
  duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
  out-of-order packets: 0 (0 bytes)
  packets with data after window: 0 (0 bytes)
  packets after close: 0
  ACK packets: 3531 (795048 bytes)
  duplicate ACK packets: 33, ACK packets for unsend data: 0

Sent packets:
  Total: 4058
  urgent packets: 0
  control packets: 50
  window probe packets: 3, window update packets: 11
```

data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
ACK-only packets: 150 (52 delayed)
unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:

entries added to syncache: 12
syncache entries retransmitted: 0
duplicate SYN packets: 0
reply failures: 0
successfully build new socket: 12
bucket overflows: 0
zone failures: 0
syncache entries removed due to RST: 0
syncache entries removed due to timed out: 0
ACK checked by syncache or syncookie failures: 0
syncache entries aborted: 0
syncache entries removed due to bad ACK: 0
syncache entries removed due to ICMP unreachable: 0
SYN cookies sent: 0
SYN cookies received: 0

SACK related statistics:

SACK recoveries: 1
SACK retransmitted segments: 0 (0 bytes)
SACK blocks (options) received: 0
SACK blocks (options) sent: 0
SACK scoreboard overflows: 0

Other statistics:

retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
persist timeout: 0
keepalive timeout: 21, keepalive probe: 0
keepalive timeout, so connections disconnected: 0
fin_wait_2 timeout, so connections disconnected: 0
initiated connections: 29, accepted connections: 12, established connections:

23

closed connections: 50051 (dropped: 0, initiated dropped: 0)
bad connection attempt: 0
ignored RSTs in the window: 0
listen queue overflows: 0
RTT updates: 3518(attempt segment: 3537)
correct ACK header predictions: 0
correct data packet header predictions: 568
resends due to MTU discovery: 0
packets dropped with MD5 authentication: 0
packets permitted with MD5 authentication: 0

表1-6 display tcp statistics 命令显示信息描述表

	字段	描述
Received packets:	Total	接收的报文总数
	packets in sequence	按顺序到达的报文数，括号中为字节数
	window probe packets	接收的窗口探测报文数
	window update packets	接收的窗口更新报文数
	checksum error	接收的校验和错误报文数
	offset error	接收的偏移量错误报文数
	short error	接收的报文长度太短的报文数
	packets dropped for lack of memory	由于内存不足而被丢弃的报文数
	packets dropped due to PAWS	由于PAWS（防止序号回绕）而被丢弃的报文数
	duplicate packets	接收的完全重复报文数，括号中为字节数
	partially duplicate packets	接收的部分重复报文数，括号中为字节数
	out-of-order packets	接收的顺序错乱的报文数，括号中为字节数
	packets with data after window	落在接收窗口外的报文数，括号中为字节数
	packets after close	在连接关闭后到达的报文数
	ACK packets	接收的ACK确认报文数，括号中为字节数
	duplicate ACK packets	接收的重复的ACK确认报文数
ACK packets for unsend data	接收的确认未发送数据的ACK报文数	
Sent packets:	Total	发送的报文总数
	urgent packets	发送的紧急数据报文数
	control packets	发送的控制报文数，括号中为包含的重传数据报文数
	window probe packets	发送的窗口探测报文数
	window update packets	发送的窗口更新报文数
	data packets	发送的数据报文数，括号中为字节数
	data packets retransmitted	重发的数据报文数，括号中为字节数
	ACK-only packets	发送的ACK报文数，括号中为延迟ACK报文数
	unnecessary packet retransmissions	报文非必要重传次数
Syncache/syncookie related statistics:	entries added to syncache	添加的syncache对象数
	syncache entries retransmitted	重传的syncache对象数
	duplicate SYN packets	重复的SYN报文数

	字段	描述
	reply failures	回复失败的报文数
	successfully build new socket	创建子socket成功数
	bucket overflows	bucket溢出次数
	zone failures	内存分配失败次数
	syncache entries removed due to RST	由于收到RST（复位连接）报文段而删除的syncache对象个数
	syncache entries removed due to timed out	定时器超时且重传次数超过限制时syncache对象删除数
	ACK checked by syncache or syncookie failures	接收到ACK报文时查找syncache处理失败数
	syncache entries aborted	创建子socket失败数
	syncache entries removed due to bad ACK	由于bad ACK而删除的syncache对象数
	syncache entries removed due to ICMP unreachable	由于接收到ICMP差错报文导致删除的syncache对象数
	SYN cookies sent	SYN cookie发送数
	SYN cookies received	SYN cookie接收数
SACK related statistics	SACK recoveries	通过SACK进行恢复的次数
	SACK retransmitted segments	通过SACK进行重传的报文段个数，括号中为字节数
	SACK blocks (options) received	接收到的带选择性ACK选项的报文数
	SACK blocks (options) sent	发送的带选择性ACK选项的报文数
	SACK scoreboard overflows	本地维护的对端缺失报文段记录队列溢出次数
Other statistics	retransmitted timeout	重传定时器超时次数
	connections dropped in retransmitted timeout	重传次数超过限制而丢弃的连接数
	persist timeout	持续定时器超时次数
	keepalive timeout	存活定时器超时次数
	keepalive probe	发送的存活探测报文数
	keepalive timeout, so connections disconnected	存活定时器超时而中断的连接数
	fin_wait_2 timeout, so connections disconnected	Fin wait 2定时器超时而中断的连接数
	initiated connections	发起连接次数
	accepted connections	接受连接次数
established connections	已建立连接数	

字段	描述
closed connections(dropped: 0, initiated dropped: 0)	已关闭连接数目，括号中为意外丢弃连接数（收到对端SYN之后）、主动连接失败数（收到对端SYN之前）
bad connection attempt	接收到的错误连接报文数
ignored RSTs in the window	窗口中忽略的RST报文数
listen queue overflows	监听队列溢出次数
RTT updates(attempt segment)	RTT更新次数，括号中为发送的报文数
correct ACK header predictions	ACK通过首部预测算法的次数
correct data packet header predictions	数据报文通过首部预测算法的次数
resends due to MTU discovery	由于MTU发现而重传的报文数
packets dropped with MD5 authentication	MD5验证丢弃报文数
packets permitted with MD5 authentication	MD5验证通过报文数

【相关命令】

- **reset tcp statistics**

1.1.7 display tcp verbose

display tcp verbose 命令用来显示 TCP 连接详细信息。

【命令】

display tcp verbose [slot slot-number [pcb pcb-index]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 TCP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 TCP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display tcp verbose 命令用来显示 TCP 连接的详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号等，以及 TCP 连接的源 IP 地址及端口号、目的 IP 地址及端口号、状态等信息。

【举例】

显示 TCP 连接详细信息。

```
<Sysname> display tcp verbose
TCP inpcb number: 1(tcpcb number: 1)

Slot: 6
Creator: telnetd_mips[199]
State: ISCONNECTED
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 65700 / 1 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
Type: 1
Protocol: 6
Connection info: src = 192.168.20.200:23 , dst = 192.168.20.14:4181
Inpcb flags: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Connection state: ESTABLISHED
Send VRF: 0x0
Receive VRF: 0x0
```

表1-7 display tcp verbose 命令显示信息描述表

字段	描述
TCP inpcb number	TCP类型internet协议控制块个数
tcpcb number	TCP控制块个数（处于TIME_WAIT状态的TCP则没有此计数）
Slot	设备在IRF中的成员编号
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： <ul style="list-style-type: none">• NOFDREF：用户已经关闭• ISCONNECTED：连接已经建立• ISCONNECTING：正在建立连接• ISDISCONNECTING：正在断开连接• ASYNC：异步方式• ISDISCONNECTED：连接已经断开• PROTOREF：协议强关联• N/A：不处于上述状态

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> SO_DEBUG：记录套接字的调试信息 SO_ACCEPTCONN：server 端监听连接请求 SO_REUSEADDR：允许本地地址重复使用 SO_KEEPALIVE：协议需要查询空闲的连接 SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 SO_BROADCAST：套接字支持广播报文 SO_LINGER：套接字关闭但仍发送剩余数据 SO_OOBINLINE：带外数据采用内联方式存储 SO_REUSEPORT：允许本地端口重复使用 SO_TIMESTAMP：入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE SO_TIMESTAMPNS：和时间戳选项功能类似，时间可以精确到纳秒 SO_KEEPALIVETIME：设置空闲探测时间 N/A：没有设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> CANTSENDMORE：不能发送数据到对端 CANTRCVMORE：不能从对端接收数据 RCVATMARK：接收标记 N/A：不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> CANTSENDMORE：不能发送数据到对端 CANTRCVMORE：不能从对端接收数据 RCVATMARK：接收标记 N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> 1：SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 2：SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 3：SOCK_RAW，RAW 模式的通信方式 N/A：不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • (暂不支持) INP_SNDBYLSPV: 通过 MPLS 发送 • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL	Internet协议控制块中的生存周期，括号中为最小生存周期

字段	描述
Connection state	<p>TCP连接状态，可能的状态如下：</p> <ul style="list-style-type: none"> • CLOSED: 服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN: 服务器在等待连接请求时所处的状态 • SYN_SENT: 客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD: 服务器收到客户端连接请求时所处的状态 • ESTABLISHED: 服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT: 服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1: 客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING: 连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK: 服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2: 客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT: 客户端收到服务器的关闭连接请求后所处的状态
Send VRF	(暂不支持) 发送实例
Receive VRF	(暂不支持) 接收实例

1.1.8 display udp

display udp 命令用来显示 UDP 连接摘要信息。

【命令】

display udp [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 UDP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display udp 命令用来显示 UDP 连接摘要信息，包括本端 IP 地址及端口号、对端 IP 地址及端口号等信息。

【举例】

显示 UDP 连接摘要信息。

```
<Sysname> display udp
Local Addr:port      Foreign Addr:port      Slot PCB
```

```

0.0.0.0:69          0.0.0.0:0          1      0x0000000000000003
192.168.20.200:1024 192.168.20.14:69   1      0x0000000000000002

```

表1-8 display udp 命令显示信息描述表

字段	描述
Local Addr:port	本端IP地址及端口号
Foreign Addr:port	对端IP地址及端口号
Slot	设备在IRF中的成员编号
PCB	协议控制块索引

1.1.9 display udp statistics

display udp statistics 命令用来显示 UDP 流量统计信息。

【命令】

display udp statistics [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 UDP 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display udp statistics 命令用来显示 UDP 流量统计信息,包括接收和发送的各类 UDP 报文信息。

【举例】

显示 UDP 流量统计信息。

```

<Sysname> display udp statistics
Received packets:
  Total: 240
  checksum error: 0, no checksum: 0
  shorter than header: 0, data length larger than packet: 0
  no socket on port(unicast): 0
  no socket on port(broadcast/multicast): 240
  not delivered, input socket full: 0
Sent packets:
  Total: 0

```

表1-9 display udp statistics 命令显示信息描述表

字段		描述
Received packets:	Total	接收的UDP报文总数
	checksum error	校验和出错的报文数
	no checksum	没有校验和的报文数
	shorter than header	报文长度比报文头部短的报文数
	data length larger than packet	报文数据长度超过报文长度的报文数
	no socket on port(unicast)	端口上无socket的单播报文数
	no socket on port(broadcast/multicast)	端口上无socket的广播和组播报文数
	not delivered, input socket full	因为socket缓冲区已满而没有向上层传送的报文数
Sent packets:	Total	发送的UDP报文总数

【相关命令】

- **reset udp statistics**

1.1.10 display udp verbose

display udp verbose 命令用来显示 UDP 连接详细信息。

【命令】

display udp verbose [slot slot-number [pcb pcb-index]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 UDP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 UDP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

display udp verbose 命令用来显示 UDP 连接的详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号等，以及 UDP 连接的源 IP 地址及端口号、目的 IP 地址及端口号等信息。

【举例】

显示 UDP 连接详细信息。

```

<Sysname> display udp verbose
Total UDP socket number: 1

Slot: 6
Creator: sock_test_mips[250]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 41600 / 1 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 2
Protocol: 17
Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
Inpcb flags: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff

```

表1-10 display udp verbose 命令显示信息描述表

字段	描述
Total UDP socket number	UDP socket总数
Slot	设备在IRF中的成员编号
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： <ul style="list-style-type: none"> • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态

字段	描述
Options	<p>socket的选项，有以下几种：</p> <ul style="list-style-type: none"> • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建SIGPIPE • SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒 • N/A：没有设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/state)	<p>接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	<p>发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有：</p> <ul style="list-style-type: none"> • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	<p>使用的socket类型，类型的取值有：</p> <ul style="list-style-type: none"> • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号

字段	描述
Inpcb flags	<p>Internet协议控制块中的标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • (暂不支持) INP_SNDBYLSPV: 通过 MPLS 发送 • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb vflag	<p>Internet协议控制块中的IP版本标记，标记的取值有：</p> <ul style="list-style-type: none"> • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKETREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL	Internet协议控制块中的生存周期，括号中为最小生存周期
Send VRF	(暂不支持) 发送实例
Receive VRF	(暂不支持) 接收实例

1.1.11 ip forward-broadcast

ip forward-broadcast 命令用来配置允许接口接收和转发直连网段的定向广播报文。

undo ip forward-broadcast 命令用来禁止接口接收和转发直连网段的定向广播报文。

【命令】

ip forward-broadcast

undo ip forward-broadcast

【缺省情况】

接口禁止接收和转发直连网段的定向广播报文。

【视图】

接口视图

【缺省用户角色】

network-admin

【使用指导】

定向广播报文是指发送给特定网络的广播报文。该报文的 **IP** 地址中网络号码字段为特定网络的网络号，主机号码字段为全 1。

接口接收和转发直连网段的定向广播报文包括以下几种情况：

- 在接收定向广播报文的情况下，如果在接口上配置了此命令，设备允许接收此接口直连网段的定向广播报文。
- 在转发定向广播报文的情况下，如果在接口上配置了此命令，设备从其他接口接收到目的地地址为此接口直连网段的定向广播报文时，会从此接口转发此类报文。

黑客可以利用定向广播报文来攻击网络系统，给网络的安全带来了很大的隐患。但在某些应用环境下，设备接口需要接收或转发这类定向广播报文，例如使用 **UDP Helper** 功能，将广播报文转换为单播报文发送给指定的服务器。

在上述情况下，用户可以通过命令配置接口允许接收和转发直连网段的定向广播报文。

【举例】

配置允许 VLAN 接口 2 接收和转发面向直连网段的定向广播报文。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast
```

1.1.12 ip icmp error-interval

ip icmp error-interval 用来配置指定时间内发送 ICMP 差错报文的最大个数。

undo ip icmp error-interval 用来恢复缺省情况

【命令】

ip icmp error-interval *milliseconds* [*bucketsize*]

undo ip icmp error-interval

【缺省情况】

令牌桶容量为 10，令牌桶的刷新周期为 100 毫秒，即每一个刷新周期内最多可以发送 10 个 ICMP 差错报文。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

milliseconds: 令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMP 差错报文的发送。

bucketsize: 令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【使用指导】

如果网络中短时间内发送的 ICMP 差错报文过多，将可能导致网络拥塞。为了避免这种情况，用户可以控制设备在指定时间内发送 ICMP 差错报文的最大个数，目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量，即令牌桶中可以同时容纳的令牌数；同时可以设置令牌桶的刷新周期，即每隔多长时间将令牌桶内的令牌个数刷新为所配置的容量。一个令牌表示允许发送一个 ICMP 差错报文，每当发送一个 ICMP 差错报文，则令牌桶中减少一个令牌。如果连续发送的 ICMP 差错报文超过了令牌桶的容量，则后续的 ICMP 差错报文将不能被发送出去，直到按照所设置的刷新频率将新的令牌放入令牌桶中。

【举例】

配置设备每 200 毫秒最多发送 40 个 ICMP 差错报文。

```
<Sysname> system-view
[Sysname] ip icmp error-interval 200 40
```

1.1.13 ip icmp fragment discarding

ip icmp fragment discarding 命令用来关闭 ICMP 分片报文转发功能。

undo ip icmp fragment discarding 命令用来开启 ICMP 分片报文转发功能。

【命令】

```
ip icmp fragment discarding
undo ip icmp fragment discarding
```

【缺省情况】

ICMP 分片报文转发功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

为了防止 ICMP 分片报文攻击，用户可以关闭设备的 ICMP 分片报文转发功能，对于收到的 ICMP 分片报文不进行转发。

【举例】

关闭 ICMP 分片报文转发功能。

```
<Sysname> system-view
```

```
[Sysname] ip icmp fragment discarding
```

1.1.14 ip icmp source

ip icmp source 命令用来配置 ICMP 报文指定源地址功能。

undo ip icmp source 命令用来关闭 ICMP 报文指定源地址功能。

【命令】

```
ip icmp source ip-address
```

```
undo ip icmp source
```

【缺省情况】

ICMP 报文指定源地址功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: 表示设备发送 ICMP 报文时指定的源地址。

【使用指导】

在网络中 IP 地址配置较多的情况下，收到 ICMP 报文时，用户很难根据报文的源 IP 地址判断报文来自哪台设备。为了简化这一判断过程，可以配置 ICMP 报文指定源地址功能。用户配置特定地址（如环回口地址）为 ICMP 报文的源地址，可以简化判断。

设备发送 ICMP 差错报文（TTL 超时、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

【举例】

配置设备发送 ICMP 报文时指定的源地址为 1.1.1.1。

```
<Sysname> system-view  
[Sysname] ip icmp source 1.1.1.1
```

1.1.15 ip mtu

ip mtu 命令用来配置接口上发送 IPv4 报文的 MTU。

undo ip mtu 命令用来恢复缺省情况。

【命令】

```
ip mtu mtu-size
```

```
undo ip mtu
```

【缺省情况】

没有配置接口 MTU。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

mtu-size: 接口 MTU 的大小, 对于 Release 1118P02 版本, 取值范围为 128~1500; 对于 Release 1122 及以上版本, 取值范围为 128~9216, 单位为字节。

【使用指导】

当设备使用某个接口发送报文时, 发现报文长度大于该接口的发送 IPv4 报文的 MTU, 则进行下列处理:

- 如果报文不允许分片, 则将报文丢弃;
- 如果报文允许分片, 则将报文进行分片转发。

为了减轻转发设备在传输过程中的分片和重组数据包的压力, 更高效的利用网络资源, 请根据实际组网环境设置合适的接口 MTU 值, 以减少分片的发生。

如果当前接口同时支持 **mtu** 和 **ip mtu** 命令, 则设备会以 **ip mtu** 命令配置的接口 MTU 值对报文进行分片, 不会再按照 **mtu** 命令配置的 MTU 值对报文进行分片。

【举例】

配置 VLAN 接口 100 上发送 IPv4 报文的 MTU 为 1280 字节。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip mtu 1280
```

1.1.16 ip redirects enable

ip redirects enable 命令用来开启设备的 ICMP 重定向报文的发送功能。

undo ip redirects enable 命令用来关闭设备的 ICMP 重定向报文的发送功能。

【命令】

ip redirects enable

undo ip redirects enable

【缺省情况】

ICMP 重定向报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

主机启动时, 它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时, 缺省网关会向源主机发送 ICMP 重定向报文, 通知主机重新选择正确的下一跳进行后续报文的发送。

满足下列条件时, 设备会发送 ICMP 重定向报文:

- 接收和转发数据报文的接口是同一接口;

- 被选择的路由本身没有被 ICMP 重定向报文创建或修改过；
- 被选择的路由不是设备的默认路由；
- 数据报文中没有源路由选项。

ICMP 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。

【举例】

开启设备的 ICMP 重定向报文发送功能。

```
<Sysname> system-view
[Sysname] ip redirects enable
```

1.1.17 ip ttl-expires enable

ip ttl-expires enable 命令用来开启设备的 ICMP 超时报文的发送功能。

undo ip ttl-expires enable 命令用来关闭设备的 ICMP 超时报文的发送功能。

【命令】

```
ip ttl-expires enable
undo ip ttl-expires enable
```

【缺省情况】

ICMP 超时报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMP 超时报文发送功能是在设备收到 IP 数据报文后，如果发生超时差错，则将报文丢弃并给源端发送 ICMP 超时差错报文。

设备在满足下列条件时会发送 ICMP 超时报文：

- 设备收到 IP 数据报文后，如果报文的目的地不是本地且报文的 TTL 字段是 1，则发送“TTL 超时”ICMP 差错报文；
- 设备收到目的地址为本地的 IP 数据报文的第一个分片后，启动定时器，如果所有分片报文到达之前定时器超时，则会发送“重组超时”ICMP 差错报文。

需要注意的是，关闭 ICMP 超时报文发送功能后，设备不会再发送“TTL 超时”ICMP 差错报文，但“重组超时”ICMP 差错报文仍会正常发送。

【举例】

开启设备的 ICMP 超时报文发送功能。

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

1.1.18 ip unreachable enable

ip unreachable enable 命令用来开启设备的 ICMP 目的不可达报文的发送功能。

undo ip unreachable enable 命令用来关闭设备的 ICMP 目的不可达报文的发送功能。

【命令】

```
ip unreachable enable
undo ip unreachable enable
```

【缺省情况】

ICMP 目的不可达报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ICMP 目的不可达报文发送功能是在设备收到 IP 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMP 目的不可达差错报文。

设备在满足下列条件时会发送目的不可达报文：

- 设备在转发报文时，如果在路由表中没有找到对应的转发路由，且路由表中没有缺省路由，则给源端发送“网络不可达” ICMP 差错报文；
- 设备收到目的地址为本地的数据报文时，如果设备不支持数据报文采用的传输层协议，则给源端发送“协议不可达” ICMP 差错报文；
- 设备收到目的地址为本地、传输层协议为 UDP 的数据报文时，如果报文的端口号与正在使用的进程不匹配，则给源端发送“端口不可达” ICMP 差错报文；
- 源端如果采用“严格的源路由选择”发送报文，当中间设备发现源路由所指定的下一个设备不在其直接连接的网络上，则给源端发送“源站路由失败”的 ICMP 差错报文；
- 设备在转发报文时，如果转发接口的 MTU 小于报文的长度，但报文被设置了不可分片，则给源端发送“需要进行分片但设置了不分片比特” ICMP 差错报文。

【举例】

开启设备的 ICMP 目的不可达报文发送功能。

```
<Sysname> system-view
[Sysname] ip unreachable enable
```

1.1.19 reset ip statistics

reset ip statistics 命令用来清除 IP 报文统计信息。

【命令】

```
reset ip statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 清除指定成员设备的 IP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

在某些情况下，需要统计一定时间内接口的 IP 报文统计信息，这时必须在统计开始前清除原有的统计信息，重新进行统计。

【举例】

清除 IP 报文统计信息。

```
<Sysname> reset ip statistics
```

【相关命令】

- **display ip interface**（三层技术-IP 业务命令参考/IP 地址）
- **display ip statistics**

1.1.20 reset tcp statistics

reset tcp statistics 命令用来清除 TCP 连接的流量统计信息。

【命令】

reset tcp statistics

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 TCP 连接的流量统计信息。

```
<Sysname> reset tcp statistics
```

【相关命令】

- **display tcp statistics**

1.1.21 reset udp statistics

reset udp statistics 命令用来清除 UDP 流量统计信息。

【命令】

reset udp statistics

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

```
# 清除 UDP 流量统计信息。  
<Sysname> reset udp statistics
```

【相关命令】

- **display udp statistics**

1.1.22 tcp mss

tcp mss 命令用来配置接口的 TCP 最大报文段长度。

undo tcp mss 命令用来恢复缺省情况。

【命令】

```
tcp mss value  
undo tcp mss
```

【缺省情况】

未配置接口的 TCP 最大报文段长度。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

value: TCP 最大报文段长度，取值范围为 128~2048，单位为字节。

【使用指导】

TCP 最大报文段长度（Max Segment Size, MSS）表示 TCP 连接的对端发往本端的最大 TCP 报文段的长度，目前作为 TCP 连接建立时的一个选项来协商：当一个 TCP 连接建立时，连接的双方要将 MSS 作为 TCP 报文的一个选项通告给对端，对端会记录下这个 MSS 值，后续在发送 TCP 报文时，会限制 TCP 报文的大小不超过该 MSS 值。当对端发送的 TCP 报文的长度小于本端的 TCP 最大报文段长度时，TCP 报文不需要分段；否则，对端需要对 TCP 报文按照最大报文段长度进行分段处理后再发给本端。

需要注意的是，该配置仅对新建的 TCP 连接生效，对于配置前已建立的 TCP 连接不生效。

【举例】

```
# 配置 VLAN 接口 100 上 TCP 最大报文段长度为 300 字节。  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] tcp mss 300
```


1.1.23 tcp path-mtu-discovery

tcp path-mtu-discovery 命令用来开启 TCP 连接的 Path MTU 探测功能。

undo tcp path-mtu-discovery 命令用来关闭 TCP 连接的 Path MTU 探测功能。

【命令】

tcp path-mtu-discovery [aging *age-time* | no-aging]

undo tcp path-mtu-discovery

【缺省情况】

TCP 连接的 Path MTU 探测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging *age-time*: Path MTU 的老化时间, *age-time* 的取值范围为 10~30, 单位为分钟, 缺省值为 10 分钟。

no-aging: Path MTU 不老化。

【使用指导】

开启 TCP 连接的 Path MTU 探测功能后, 新建的 TCP 连接均会携带 Path MTU 探测属性, 可以通过探测机制确定 Path MTU, 按照数据路径上的最小 MTU 组织 TCP 分段长度, 最大限度利用网络资源, 避免 IP 分片的发生。

关闭 TCP 连接的 Path MTU 探测功能后, 系统将停止所有正在运行的 Path MTU 定时器, 此后创建的 TCP 连接均无 Path MTU 探测功能, 但是对于此前已经建立的 TCP 连接, 其 Path MTU 探测功能不会被关闭。

【举例】

开启 TCP 连接的 Path MTU 探测功能, Path MTU 的老化时间为 20 分钟。

```
<Sysname> system-view  
[Sysname] tcp path-mtu-discovery aging 20
```

1.1.24 tcp syn-cookie enable

tcp syn-cookie enable 命令用来使能 SYN Cookie 功能, 防止设备受到 SYN Flood 攻击。

undo tcp syn-cookie enable 命令用来关闭 SYN Cookie 功能。

【命令】

tcp syn-cookie enable

undo tcp syn-cookie enable

【缺省情况】

SYN Cookie 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

一般情况下，TCP 连接的建立需要经过三次握手，一些恶意的攻击者利用 TCP 连接的建立过程进行 SYN Flood 攻击：攻击者向服务器发送大量请求建立 TCP 连接的 SYN 报文，而不回应服务器的 SYN ACK 报文，导致服务器上建立了大量的 TCP 半连接。从而，达到耗费服务器资源，使服务器无法处理正常业务的目的。

SYN Cookie 功能用来防止 SYN Flood 攻击。当服务器收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。服务器接收到发起者回应的 ACK 报文后，才建立连接。通过这种方式，可以避免在服务器上建立大量的 TCP 半连接，防止服务器受到 SYN Flood 攻击。

【举例】

```
# 使能 SYN Cookie 功能。
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

1.1.25 tcp timer fin-timeout

tcp timer fin-timeout 命令用来配置 TCP 的 finwait 定时器超时时间。

undo tcp timer fin-timeout 命令用来恢复缺省情况。

【命令】

```
tcp timer fin-timeout time-value
undo tcp timer fin-timeout
```

【缺省情况】

TCP finwait 定时器的超时时间为 675 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-value: TCP finwait 定时器的超时时间，取值范围为 76~3600，单位为秒。

【使用指导】

当 TCP 的连接状态为 FIN_WAIT_2 时，启动 finwait 定时器，如果在定时器超时前没有收到报文，则 TCP 连接终止；如果收到 FIN 报文，则 TCP 连接状态变为 TIME_WAIT 状态；如果收到非 FIN 报文，则从收到的最后一个非 FIN 报文开始重新计时，在超时后中止连接。

【举例】

```
# 配置 TCP finwait 定时器的超时时间为 800 秒。
```

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

1.1.26 tcp timer syn-timeout

tcp timer syn-timeout 命令用来配置 TCP 的 synwait 定时器超时时间。

undo tcp timer syn-timeout 命令用来恢复缺省情况。

【命令】

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

【缺省情况】

TCP synwait 定时器的超时时间为 75 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-value: TCP synwait 定时器的超时时间，取值范围为 2~600，单位为秒。

【使用指导】

当发送 SYN 报文时，TCP 启动 synwait 定时器，如果 synwait 超时前未收到回应报文，则 TCP 连接建立不成功。

【举例】

配置 TCP synwait 定时器的超时时间为 80 秒。

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

1.1.27 tcp window

tcp window 命令用来设置 TCP 连接的收发缓冲区大小。

undo tcp window 命令用来恢复缺省情况。

【命令】

tcp window *window-size*

undo tcp window

【缺省情况】

TCP 连接的收发缓冲区大小为 64KB。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

window-size: TCP 连接的收发缓冲区大小，取值范围为 1~64，单位为 KB（千字节）。

【举例】

设置 TCP 连接的收发缓冲区大小为 3KB。

```
<Sysname> system-view  
[Sysname] tcp window 3
```