网络协议配置命令

目 录

第 1 章 IP 寻址配置命令 1
1.1 IP 寻址配置命令 1
1.1.1 arp 1
1.1.2 arp timeout 2
1.1.3 clear arp-cache 3
1.1.4 ip address 3
1.1.5 ip directed-broadcast 4
1.1.6 ip forward-protocol udp 5
1.1.7 ip helper-address 5
1.1.8 ip host 6
1.1.9 ip proxy-arp 7
1.1.10 ip unnumbered 7
1.1.11 keepalive 8
1.1.12 ip route-cache-timeout 9
1.1.13 show arp 10
1.1.14 show hosts 11
1.1.27 show ip interface 18
第 2 章 NAT 配置命令 21
2.1 NAT 配置命令 21
2.1.1 ip nat 21
2.1.2 ip nat local-service 22
2.1.3 ip fastaccess 23
2.1.4 ip fastnat 1to1 24
2.1.5 ip nat inside destination 24
2.1.6 ip nat inside source 25
2.1.7 ip nat outside source 27
2.1.8 ip nat pool 29
2.1.9 ip nat service 30
2.1.10 ip nat translation 31
2.1.11 ip nat log 32
2.1.12 ip nat translation max-users[不再支持] 33
2.1.13 clear ip nat statistics 34
2.1.14 clear ip nat translation 35
2.1.15 show ip nat statistics 36
2.1.16 show ip nat translations 38
2.1.17 show ip nat users[不再支持] 39
2.1.18 debug ip nat 40
第 3 章 DHCP Client 配置命令 43
3.1 DHCP Client 配置命令 43
3.1.1 ip address dhcp 43
3.1.2 ip dhcp client 44
3.1.3 ip dhcp-server 45

3.1.4 show dhcp lease 46
3.1.5 show dhcp server 46
3.1.6 debug dhcp 47
第 4 章 DHCP Sever 配置命令 49
4.1 DHCPD 配置命令 49
4.1.1 ip dhcpd ping packet 49
4.1.2 ip dhcpd ping timeout 49
4.1.3 ip dhcpd write-time 50
4.1.4 ip dhcpd pool 51
4.1.5 ip dhcpd enable 51
4.1.6 ip dhcpd disable 52
4.2 DHCPD 地址池的配置命令 52
4.2.1 network 52
4.2.2 range 53
4.2.3 default-router 54
4.2.4 dns-server 54
4.2.5 domain-name 55
4.2.6 lease 55
4.2.7 netbios-name-server 56
4.2.8 host 57
4.2.9 hardware-address 57
4.2.10 client-identifier 58
4.2.11 client-name 58
4.3 DHCPD 的调试命令 59
4.3.1 debug ip dhcpd packet 59
4.3.2 debug ip dhcpd event 59
4.4 DHCPD 的管理命令 60
4.4.1 show ip dhcpd statistic 60
4.4.2 show ip dhcpd binding 61
4.4.3 show ip dhcpd pool 61
4.4.4 clear ip dhcpd statistic 62
4.4.5 clear ip dhcpd binding 62
4.4.6 clear ip dhcpd abandoned 63
第 5 章 DHCP-RELAY SNOOPING 配置命令 64
5.1.1 dhcp-relay snooping 64
5.1.2 dhcp-relay snooping vlan 65
5.1.3 dhcp-relay snooping vlan *vlan_id* max-client 65
5.1.4 dhcp snooping trust 66
5.1.5 dhcp snooping deny 66
5.1.6 show ip dhcp-relay snooping 67
5.1.7 show ip dhcp-relay snooping binding 67
5.1.8 debug ip dhcp-relay snooping 68
5.1.9 debug ip dhcp-relay event 68
5.1.10 debug ip dhcp-relay binding 69
第 6 章 IP 服务配置命令 70

6.1 IP Server 配置命令 70
6.1.1 clear tcp 70
6.1.2 clear tcp statistics 72
6.1.3 debug arp 72
6.1.4 debug ip icmp 73
6.1.5 debug ip packet 76
6.1.6 debug ip raw 80
6.1.7 debug ip rtp 81
6.1.8 debug ip tcp packet 84
6.1.9 debug ip tcp transactions 85
6.1.10 debug ip udp 87
6.1.11 ip mask-reply 88
6.1.12 ip mtu 88
6.1.13 ip redirects 89
6.1.14 ip route cache 90
6.1.15 ip source-route 91
6.1.16 ip tcp synwait-time 92
6.1.17 ip tcp window-size 92
6.1.18 ip unreachables 93
6.1.19 ip vrf forwarding 94
6.1.20 ip error-log 94
6.1.21 ip check-noncidr 95
6.1.22 show ip cache 95
6.1.23 show ip irdp 96
6.1.24 show ip sockets 97
6.1.25 show ip traffic 98
6.1.26 show tcp 99
6.1.27 show tcp brief 102
6.1.28 show tcp statistics 103
6.1.29 show tcp tcb 105
6.2 访问列表配置命令 106
6.2.1 deny 106
6.2.2 ip access-group 109
6.2.3 ip access-list 109
6.2.4 permit 110
6.2.5 ip http firewalltype 113
6.2.6 show ip access-list 113
6.2.7 imp access-list 114
6.2.8 permit <ip | any> <mac | any> 115
6.2.9 deny <ip | any> <mac | any> 115
6.2.10 imp access-group 116
6.2.11 Ip access-list extended *** massive 117
6.2.12 Ip access-list table-limit *** 117
6.2.13 Ip access-list cache-enable 118
6.3 URPF 配置命令 119
6.3.1 verify ipv4 unicast source reachable-via 119

6.4 ip fastswitch 120
6.5 FTP 配置命令 120
6.5.1 ftp-server enable 120
6.5.2 ftp-server maxlogin 121
6.5.3 ftp-server attack-defense 122
6.5.4 ftp-server anonymous-permission 122
6.5.5 ftp-server certificate 123
6.5.6 ftp-server user-group 124
6.5.7 ftp-user 124
6.5.8 privilege 125
6.6 防攻击配置命令 126
6.6.1 verify ipv4 enable 126
6.6.2 verify ipv4 filter 127
6.6.3 verify ipv4 all 128
6.6.4 verify ipv4 icmp 129
6.7 报文连续处理个数配置命令 133
6.7.1 packet-handle-pause 133
6.8 硬件优先接收匹配模式配置命令 133
6.8.1 cavium pip-watcher 133
6.9 系统 MTU 配置命令 134
6.9.1 System mtu 134

第1章　IP 寻址配置命令

1.1　IP寻址配置命令

IP 寻址配置命令包括：

- arp
- arp timeout
- clear arp-cache
- ip address
- ip directed-broadcast
- ip forward-protocol udp
- ip helper-address
- ip host
- ip proxy-arp
- ip unnumbered
- keepalive
- show arp
- show hosts
- show ip interface

1.1.1　arp

配置静态 ARP 映射，静态 ARP 映射会永久保留在 ARP 缓存中。如果要删除配置的静态 ARP 映射的话，使用 no arp 命令。

arp *ip-address hardware-address* [**alias**]

no arp *ip-address*

参数

参数	参数说明
ip-address	本地数据链路接口的IP地址。
hardware-address	本地数据链路接口的物理地址。
alias	(可选)路由器回答对这一IP地址的ARP请求，就象是本身拥有这个IP地址。

缺省

ARP 缓存中不存在永久的静态 ARP 映射。

命令模式

全局配置态

使用说明

一般的主机都可以支持动态 ARP 解析，所以一般不需要用户特地为主机配置静态 ARP 映射。

示例

下面的这条命令配置 IP 地址为 1.1.1.1 的主机的 MAC 地址为 00:12:34:56:78:90。

arp 1.1.1.1 00:12:34:56:78:90

相关命令

clear arp-cache

1.1.2 arp timeout

配置 ARP 缓存中动态 ARP 表项的存在时间。如果要恢复到缺省值的话，使用 **no arp timeout** 或 **default arp timeout** 命令。

arp timeout seconds

no arp timeout

default arp timeout

参数

参数	参数说明
seconds	ARP缓存中动态ARP表项的存在时间（秒）。0 表示在这个接口动态解析得到的ARP缓存不会被超时释放。

缺省

14400 秒 (4 小时)

命令模式

接口配置态

使用说明

如果在不使用 ARP 的接口上进行配置，则配置无效。show interface 命令将显示在这个接口上配置的 ARP 表项超时时间，显示如下：

ARP type: ARPA, ARP timeout 04:00:00

示例

下面这条命令在接口 Ethernet 1/0 上配置动态 ARP 映射的生存时间是 900 秒，以便使 ARP 缓存更快地刷新。

```
interface ethernet 1/0
arp timeout 900
```

相关命令

show interface

1.1.3 clear arp-cache

清除所有动态 ARP 缓存。

clear arp-cache

参数

命令没有参数或关键字。

命令模式

管理态

示例

下面的命令清除所有的动态 ARP 缓存。

clear arp-cache

相关命令

Arp

1.1.4 ip address

配置接口 IP 地址，同时设置网络掩码。目前已经不再严格区分 A,B,C 类 IP 地址，但是，不能使用多播地址和广播地址（主机部分全“1”）。除了以太网，其它类型的多个接口可以在同一个网段上。但是，以太网接口所配置的网段不能和其它任意类型的接口相同，除了无编号接口。一个接口上一般都可以配置一个主地址和无限多个从属地址。从属地址只能在配置了主地址后才可以配置，从属地址全部删除之后才可以删除主地址。系统本身生成的 IP 报文，如果上层应用没有指定源地址，路由器将使用发出接口上配置的与网关在同一网段上的 IP 地址作为报文的源地址，如果不能确定这个 IP 地址（例如接口路由），则采用发出接口的主地址。如果一个接口没有配置 IP 地址，而且也不是无编号接口（unnumbered 接口），则这个接口不处理 IP 报文。

如果要删除 IP 地址，或者停止某个接口对 IP 报文的处理，可以使用 no ip address 命令清除接口上的某个或所有 IP 地址。

ip address *ip-address mask* [**secondary**]

no ip address *ip-address* **mask**

no ip address

参数

参数	参数说明
ip-address	IP 地址。

mask	IP 网络掩码。
secondary	(可选) 指明配置的是IP从属地址，如果没有指明，则配置的是IP主地址。

缺省

接口上不配置任何 IP 地址。

命令模式

接口配置态

使用说明

如果路由器在某个物理网段上配置了从属 IP 地址，其它同一物理网段上的系统也必须配置相同逻辑网段的从属地址，否则容易很快就引起路由循环。

当使用 OSPF 协议时，要确保一个接口上的从属地址和它的主地址在同一个 OSPF area 中。

示例

下列命令在 ethernet1/0 接口上配置主地址 202.0.0.1，网络掩码 255.255.255.0，另外配置了两个 IP 从属地址 203.0.0.1 和 204.0.0.1。

```
interface ethernet1/0
ip address 202.0.0.1 255.255.255.0
ip address 203.0.0.1 255.255.255.0 secondary
ip address 204.0.0.1 255.255.255.0 secondary
```

1.1.5 ip directed-broadcast

转发 IP 定向广播，并将报文以物理广播的形式发送。

ip directed-broadcast [*access-list-namer*]

no ip directed-broadcast

参数

参数	参数说明
access-list-name	（可选）访问表名称。如果定义了访问表，只有访问表允许的广播报文被转发。

缺省

缺省情况下，不转发 IP 定向广播。

命令模式

接口配置态

示例

下面的例子在接口 ethernet1/0 上配置转发 IP 定向广播。

```
interface ethernet 1/0
ip directed-broadcast
```

1.1.6 ip forward-protocol udp

当接口上配置了 ip helper-address 后，用于指定对哪些 UDP 协议有限广播报文进行转发。

ip forward-protocol udp [*port*]

no ip forward-protocol udp [*port*]

default ip forward-protocol udp

参数

参数	参数说明
port	（可选）需要被转发的UDP报文的目的端口。

缺省

转发 NETBIOS 名字服务（Name Service）报文。

命令模式

全局配置态

使用说明

目前缺省转发 NETBIOS 名字服务报文，如果要求不转发 NETBIOS 名字服务报文，可以使用下列任一命令：

no ip forward-protocol udp netbios-ns

no ip forward-protocol udp 137

使用下面的命令停止转发所有 UDP 有限广播报文：

no ip forward-protocol udp

示例

```
Router_config#ip forward-protocol udp 137
```

相关命令

ip helper-address

1.1.7 ip helper-address

将 IP 定向广播报文转发到命令指定的 IP 帮助地址，可以是单目或者是广播地址。每个接口可以配置多个帮助地址。ip helper-address *address*

no ip helper-address [*address*]

参数

参数	参数说明
address	IP 帮助地址。

缺省

未配置 IP 帮助地址。

命令模式

接口配置态

使用说明

该命令在 X.25 接口上不起作用，因为路由器不能辨别出物理广播。

示例

下面的命令在接口 ethernet1/0 上配置 IP 帮助地址 1.0.0.1。

```
interface ethernet 1/0
ip helper-address 1.0.0.1
```

相关命令

ip forward-protocol udp

1.1.8 ip host

定义静态主机名称—地址映射。如果要删除主机名称—地址映射，使用 no ip host 命令。

ip host name address

no ip host *name*

参数

参数	参数说明
name	主机名称。
Address	IP地址。

缺省

没有配置任何映射。

命令模式

全局配置态

示例

下面的例子配置 IP 地址为 202.96.1.3 的主机名称是 dns-server。

ip host dns-server 202.96.1.3

1.1.9 ip proxy-arp

在接口上进行代理 ARP。如果要关闭这项功能，使用 no ip proxy arp 命令。

ip proxy-arp

no ip proxy-arp

参数

命令没有参数或关键字。

缺省

进行代理 ARP。

命令模式

接口配置态

使用说明

当路由器收到 ARP 请求时，如果路由器有到被请求 IP 地址的路由，且路由接口和收到请求的接口不同，路由器将以自己的 MAC 地址发出 ARP 响应，然后，在收到实际数据报文时，进行转发。这样，即使一台主机不完全了解网络的拓扑结构，或者没有配置准确的路由，也能和远端通信。对它来说，远端主机就和它直接连接在同一个物理子网中。

如果主机需要路由器提供这项服务，它和路由器必须在同一个 IP 网络中，或者，至少它的 IP 地址必须能够使路由器认为它们在同一个 IP 子网中，也就是说，可以使用不同的掩码。否则，路由器将不提供这项服务。

示例

下面的例子在接口 ethernet1/0 上打开代理 ARP 功能：

interface ethernet 1/0
ip proxy-arp

1.1.10 ip unnumbered

配置一个接口为无编号接口，可以不配置 IP 地址就开启 IP 处理功能。要停止这个接口上的 IP 处理，使用 no ip unnumbered 命令。

ip unnumbered *type number*

no ip unnumbered

参数

参数	参数说明

type number	另一个配置了IP地址的接口的类型和编号。这个接口不可以是使用其它接口IP地址的无编号接口。

缺省

不启动这项功能。

命令模式

接口配置态

使用说明

对于点到点链路接口来说，可以不配置独有的 IP 地址，而是使用这条命令在这个接口上启动 IP 处理，并指定借用其它接口上的有效 IP 地址作为这个接口发出报文的源地址，以便节省 IP 地址。这样的点到点接口称为无编号（unnumbered）接口。无编号接口上生成的 IP 报文，例如路由更新报文，将使用命令中指定的接口上配置的有效 IP 地址。它还用这一地址确定哪些路由进程在该接口上发送更新报文。但是，有下列限制：

(1) 使用 HDLC, PPP, LAPB, SLIP 和帧中继封装的串行接口和隧道接口可以使用该条命令配置成无编号接口。但是，X.25 和 SMDS 接口不能使用这条命令。

(2) 无法通过 ping 命令检测这个接口是否正常工作。可以使用 SNMP 远程检测这个接口的状态。

这条命令根据 RFC 1195 中关于接口可以不配置有效 IP 地址的规定实现。

在不同的主网之间的使用其它接口 IP 地址的串行链路，必须小心对待：任何运行在这条链路上的路由协议不能广播任何有关各自子网的信息。

示例

下面的命令将接口 serial0/0 配置成无编号接口，使用接口 ethernet0/1 上配置的有效 IP 地址 1.0.0.1 作为这个接口上发出报文的源地址：

```
interface ethernet 0/1
ip address 1.0.0.1 255.255.255.0
interface serial 0/0
ip unnumbered ethernet 1/0
```

1.1.11 keepalive

测试主机的可到达性和网络的连通性。通过发送 ICMP 回应请求报文给对方，但不等待对方的 ICMP 回应应答报文。

keepalive [**group** *group-id*] [**source** *source-address*] [**interval** interval-time] [**number** *number*] **destination** *destination-address*

参数

参数	参数说明
group *group-id*	可以配置多条 keepalive 命令，命令之间以group-id区分。缺省：0
source	设置报文采用的源IP地址。

source-address	缺省：发送接口的主IP地址。
interval *interval-time*	每次报文发送之间的间隔,以秒为单位。缺省：1秒
number *number*	每次报文发送的个数。缺省：5。
destination *destination-address*	目的主机。

命令模式

管理态和全局配置态

使用说明

keepalive 命令支持广播地址和多播地址。如果是有限广播（255.255.255.255）或者是多播地址，将在所有支持广播或者是多播的可用接口上发送 ICMP 回应请求报文。

该命令不等待 ICMP 报文的应答，它只是定时向目的地址发送指定数目的 ICMP 报文。

示例

以下配置了两条 keepalive 命令。

配置每 10 秒钟以源地址 192.168.20.230 向目的地址 192.168.20.1 发送 10 个 ICMP request 报文。报文的发送端口由目的地址 192.168.20.1 和路由协议共同决定。

keepalive group 1 destination 192.168.20.1 source 192.168.20.230 interval 10 number 10

配置每 1 秒钟(默认值)以源地址 172.16.20.232 向目的地址 172.16.20.5 发送 5 个(默认值) ICMP request 报文。报文的发送端口由目的地址 172.16.20.2 和路由协议共同决定。

keepalive group 2 destination 172.16.20.2 source 172.16.20.232

1.1.12 ip route-cache-timeout

该命令用于设置路由缓存老化时间。

(no)ip route-cache-timeout *timeout-value*

参数

参数	参数说明
timeout-value	路由缓存老化时间。单位：5秒，缺省：1（即老化时间为5秒）

命令模式

全局配置态

使用说明

该命令用于设置路由缓存老化时间。老化时间设置越长，那么对于同一条数据流（源地址、目的地址相同）而言，用于查找路由的时间越短，所以当通过路由器的数据流条数较少（小于 1 万条）且数据流构成较为固定时，适当延长路由缓存老化时间，能够提高

路由器转发效率。但是，当数据流条数较大（大于 1 万条）且数据流构成不固定时，老化时间过长，有可能造成资源浪费，反而造成路由器的转发效率低下。所以一般情况下推荐使用缺省值（即用户不用设置路由器缓存老化时间）。对于我公司 1705 系列宽带路由器，在使用双线路情况下，老化时间推荐设置为 16（即 80 秒）。

示例

下面的命令设置路由缓存老化时间为 10 秒：

```
router#config
router_config#
router_config#ip route-cache-timeout 2
```

下面的命令删掉配置的路由缓存老化时间 10 秒：

```
router#config
router_config#
router_config#no ip route-cache-timeout 2
```

此时将恢复缺省值 1。

1.1.13 show arp

显示所有 ARP 表项，包括接口 IP 地址的 ARP 映射，用户配置的静态 ARP 映射，动态 ARP 映射。

show arp

参数

无

命令模式

管理态

使用说明

显示的信息包括：

参数	参数说明
Protocol	协议，与物理地址映射的网络地址的类型，例如IP。
Address	地址，与物理地址相映射的网络地址，如IP地址。
Age	生存时间，ARP表项从生成到现在的时间，以分钟为单位。路由器使用这条ARP表项不会影响这个值。
Hardware Address	物理地址，与网络地址对应的物理地址，对于尚未解析完成的表项为空。
Type	类型，表示接口使用的报文封装类型，包括ARPA，SNAP等。
Interface	接口，与这个网络地址相关联的接口。

示例

下面的命令显示 ARP 缓存：

```
router#show arp
Protocol   IP Address        Age(min)  Hardware Address    Type   Interface
  IP       192.168.20.77        11     00:30:80:d5:37:e0   ARPA   Ethernet1/0
  IP       192.168.20.33         0       Incomplete
  IP       192.168.20.22         -     08:00:3e:33:33:8a   ARPA   Ethernet1/0
  IP       192.168.20.124        0     00:a0:24:9e:53:36   ARPA   Ethernet1/0
  IP       192.168.0.22          -     08:00:3e:33:33:8b   ARPA   Ethernet1/1
```

1.1.14 show hosts

显示主机名—地址缓存中的所有表项。

show hosts

参数

命令没有参数或关键字。

命令模式

管理态

示例

下面的命令显示所有主机名称/地址映射：

show hosts

相关命令

clear host

1.1.15 arp learn-strict

设置路由器严格学习 ARP，只学习自己请求的 ARP。如果要恢复默认模式，使用 no arp learn-strict 命令。

arp learn-strict

no arp learn-strict

参数

该命令没有参数或关键字

缺省

不启用严格学习 ARP

命令模式

端口配置态

使用说明

启用严格学习 ARP 后，可以防止网络 ARP 攻击——网络主机不断更新路由器 ARP 表项。

示例

下面的例子启用 ARP 严格学习：

Router_config_g0/0#arp learn-strict

1.1.16 arp source-filter

设置路由器 ARP 源地址过滤，将对 ARP 报文中源地址进行过滤。如果要恢复默认模式，使用 no arp source-filter 命令。

arp source-filter

no arp source-filter

参数

该命令没有参数或关键字

缺省

不启用 ARP 源地址过滤

命令模式

端口配置态

使用说明

启用 ARP 源地址过滤，会根据 ARP 报文中的源地址查找路由，如果目的端口不是本端口，将丢弃该 ARP 报文。

示例

下面的例子启用 ARP 源地址过滤：

Router_config_g0/0#arp source-filter

1.1.17 arp timeout

设置路由器 ARP 老化时间。如果要恢复默认配置，使用 no arp timeout 命令。

arp timeout <seconds>

no arp timeout

参数

〈10-4294967〉

缺省

180 秒

命令模式

端口配置态

使用说明

修改 ARP 的老化时间。

示例

下面的例子启用 ARP 源地址过滤：

Router_config_g0/0#arp timeout 10

1.1.18 arp dynamic

设置路由器动态学习 ARP。如果要取消设置动态学习 ARP，使用 no arp dynamic 命令。

arp dynamic

no arp dynamic

参数

该命令没有参数或关键字

缺省

启用 ARP 动态学习

命令模式

端口配置态

使用说明

启用 ARP 动态学习，收到 ARP 报文，根据源地址 IP&MAC 更新 ARP 表项。

示例

下面的例子禁用 ARP 动态学习：

Router_config_g0/0#no arp dynamic

1.1.19 arp proxy

设置路由器 ARP 代理。如果要取消设置 ARP 代理，使用 no arp proxy 命令。

arp proxy <all | range>

no arp proxy <all | range>

参数

all：代理所有 IP 地址

range：格式为 ip & mask 的方式指定 IP 地址范围。

缺省

禁用 ARP 代理

命令模式

端口配置态

使用说明

启用 ARP 代理，路由器将响应代理 IP 的 ARP 请求。

示例

下面的例子设置 ARP 代理：

Router_config_g0/0#arp proxy all

1.1.20 arp scan

设置路由器 ARP 扫描。如果要取消设置 ARP 扫描，使用 no arp scan 命令。

arp scan <all | range>

no arp scan <all | range>

参数

all：扫描所有 IP 地址

range：格式为 ip & mask 的方式指定 IP 地址范围。

缺省

不启用 ARP 扫描

命令模式

端口配置态

使用说明

启用 ARP 扫描，路由器将主动请求扫描范围内的 IP 地址，形成静态 ARP 表项。

示例

下面的例子设置 ARP 代理：

Router_config_g0/0#arp scan all

1.1.21 arp guard

设置路由器 ARP 防攻击。如果要取消设置 ARP 保护，使用 no arp guard 命令。

arp guard

no arp guard

参数

无

缺省

禁用 ARP 防攻击

命令模式

端口配置态

使用说明

启用 ARP 防攻击，将检查 ARP 的合法性，丢弃非法报文。

示例

下面的例子设置 ARP 防攻击：

Router_config_g0/0#arp guard

1.1.22 arp guard rate-limit

设置路由器 ARP 报文限速。如果要恢复默认 ARP 限速，使用 no arp guard rate-limit 命令。

arp guard rate-limit <num>

no arp guard rate-limit

参数

每秒接收到 ARP 个数

缺省

1000

命令模式

端口配置态

使用说明

启用 ARP 限速，将统计收到的 ARP 个数，丢弃超过阀值的 ARP 报文。

示例

下面的例子设置 ARP 防攻击：

Router_config_g0/0#arp guard rate-limit 500

1.1.23 arp free-arp

设置路由器定时发送免费 ARP。如果要取消定时发送免费 ARP，使用 no arp free-arp 命令。

arp free-arp <time>

no arp free-arp

参数

0~600 (0.1 秒)

缺省

不定时发送免费 ARP

命令模式

端口配置态

使用说明

启用定时发送免费 ARP。

示例

下面的例子设置定时发送 ARP：

Router_config_g0/0#arp free-arp 100

1.1.24 arp <ip> <mac>

设置路由器静态 ARP。如果要取消定静态 ARP，使用 no arp <ip> <mac>命令。

arp <ip> <mac>

no arp <ip> <mac>

参数

Ip:格式为 a.b.c.d

Mac:格式为 hh:hh:hh:hh:hh:hh

缺省

无

命令模式

全局配置态

使用说明

启用静态 ARP 后，路由器将不请求相应 IP 的 ARP，且不会被动态修改。

示例

下面的例子设置静态 ARP：

Router_config#arp 1.1.1.1 00:a0:0c:13:64:7d

1.1.25 show arp

显示 ARP 表项。

Show arp

参数

无

缺省

无

命令模式

全局配置态

使用说明

显示当前的 ARP 表项。

示例

下面的例子显示 ARP 表项：

```
Router_config#show arp

##'M': manual 'B':bind 'S':static 'D':dynamic##
There are 1 ARP Entries Totally
Proto Address          Age(s) Hardware Address     Type   Interface
 IP    1.1.1.160         -      00:a0:0c:13:64:7d   --D    GigaEthernet0/1
```

1.1.26 clear arp

清除 ARP 表项。

Show arp

参数

无

缺省

无

命令模式

全局配置态

使用说明

清除当前的 ARP 表项。

示例

下面的例子清除 ARP 表项：

```
Router_config#clear arp
```

1.1.27 show ip interface

显示接口上的 IP 配置。

show ip interface [*type number*]

参数

参数	参数说明
type	(可选) 接口类型。
number	(可选) 接口编号。

命令模式

管理态

使用说明

如果接口的链路层可以有效收发数据，它就是一个可用接口，状态是“Protocol Up”。如果在这个接口上配置 IP 地址，路由器将在路由表中添加一条直连路由。如果链路层协议断开，也就是“Protocol Down”，这条直连路由将被删除。如果指定接口类型和编号，只显示指定接口信息。否则，显示所有接口的 IP 配置信息。

示例

下面的命令显示接口 e0/1 上的 IP 配置：

```
Router#show ip interface e0/1
   Ethernet1/0 is up, line protocol is up
    IP address : 192.168.20.167/24
      Broadcast address : 192.168.20.255
      Helper address : not set
      MTU : 1500(byte)
      Forward Directed broadcast : OFF
      Multicast reserved groups joined:
        224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
        224.0.0.1
      Outgoing ACL : not set
      Incoming ACL : not set
      IP fast switching : ON
      IP fast switching on the same interface : OFF
      ICMP unreachables : ON
      ICMP mask replies : OFF
      ICMP redirects : ON
```

显示说明：

域	描述
Ethernet1/0 is up	如果接口硬件可用，接口被标为“up”。 如果接口可用，它的硬件和线路协议都必须是up的。
line protocol is up	如果接口可以提供双向通信，它的线路协议被标为“up”。如果接口可用，接口硬件和线路协议都必须是up的。
IP address	接口IP地址和网络掩码。
Broadcast address	显示广播地址。
MTU	显示接口设置的IP MTU。
Helper address	显示帮助地址。

Directed broadcast forwarding	接口是否转发定向广播报文。
Multicast reserved groups joined	接口加入的多播组。
Outgoing ACL	接口使用的输出访问控制表。
Incoming ACL	接口使用的输入访问控制表。
IP fast switching	路由器在该端口上是否启动快速转发
Proxy ARP	接口是否支持代理ARP。
ICMP redirects	接口是否发出ICMP重定向报文。
ICMP unreachables	接口是否发出ICMP不可到达报文。
ICMP mask replies	接口是否发出ICMP掩码应答报文。

第2章 NAT 配置命令

2.1 NAT配置命令

NAT 配置命令包括：

- ip nat
- ip nat local-service
- ip nat enable-peek
- ip nat inside destination
- ip nat inside source
- ip nat outside source
- ip nat pool
- ip nat translation
- clear ip nat statistics
- clear ip nat translation
- show ip nat statistics
- show ip nat translations
- debug ip nat

2.1.1 ip nat

ip nat {**inside | outside | mss** }

no ip nat {**inside | outside | mss** *MSS-value*}

参数

参数	参数说明
inside	表明接口连接到内部网络（网络服从NAT翻译）
outside	表明接口连接到外部网络（网络服从NAT翻译）
mss *MSS-value*	设置MSS值为*MSS-value*（必须先配有ip nat outside）

缺省

离开或到达这个接口的通信量不服从 NAT。

命令模式

接口配置态

使用说明

只有那些在“内部”和“外部”接口之间传送的报文才可以被翻译。必须为每个想使用 NAT 的边界路由器至少指定一个内部接口和一个外部接口。

使用 IP NAT 接口配置命令来指定来自接口的或发往接口的通信量服从 NAT（网络地址翻译），如果想禁止接口的翻译功能，使用这个命令的 NO 形式。

注意：

ip nat mss 命令只能配在 ip nat outside 的接口下，它的作用是修改从内部网出去的带有 SYN 标志的 TCP 报文选项中的 MSS（Maximum Segment Size）值。如果想禁止该接口修改 MSS 值的功能，使用这个命令的 NO 形式。

示例

下面的例子把来自 192.168.1.0 或 192.168.2.0 网络编址的内部主机间进行通信的 IP 地址翻译为 171.69.233.208/28 网络中全局唯一的 IP 地址，并且修改 MSS 为 1432 值。

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
  ip nat mss 1432
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
.permit 192.168.2.0 255.255.255.0
!
```

2.1.2 ip nat local-service

ip nat local-service {**icmp** | **udp** | **tcp** } **disable**

no ip nat local-service {**icmp** | **udp** | **tcp** } **disable**

参数

参数	参数说明
icmp	Icmp 报文。
udp	udp报文。
tcp	tcp报文。

缺省

无

命令模式

接口配置态

使用说明

此命令应用于 PAT 规则。默认情况下，在标记为 NAT 外部端口的路由器接口，允许所有访问路由器本地的 icmp/udp/tcp 报文。该命令可以有限的防止外部网络用户对路由器的，恶意攻击，当然也丢弃了正常的访问路由器的报文。

如果想某标记为 NAT 外部端口的路由器接口禁止接收访问本地的 icmp/udp/tcp 报文，可以在端口状态下配置如下命令，使用这个命令的 NO 形式可以恢复默认状态。

注意：

此命令只能配置标记为 NAT 外部端口所在的路由器接口下，并只能使本接口禁止接收 icmp/udp/tcp 本地报文。

2.1.3 ip fastaccess

ip fastaccess deny {**tcp** | **udp** | **icmp**} {*port number*}

no ip fastnat deny {**tcp** | **udp** | **icmp**} {*port number*}

参数

参数	参数说明
deny	定义阻止包的规则
tcp	定义阻止TCP包的规则
udp	定义阻止UDP包的规则
icmp	定义阻止ICMP包的规则
Port number	TCP/UDP端口号，范围为1~10000

缺省

无

命令模式

接口配置态

使用说明

由于 ip fastaccess 只能基于传输层限制报文转发，如果需要基于 IP 地址限制，则需要用到一般访问列表

建议：如果需要使用一般访问列表限制内网用户，如果使用到动态 NAT 规则，则强烈建议利用 NAT 所用的访问列表。特别对于那些需要定义非常多规则的访问列表，这样可以显著提高性能。

2.1.4 ip fastnat 1to1

ip fastnat 1to1 outside {*interface-type number*} [**backup-outside** {*interface-type number*}] **inside** {*interface-type number*} [**privateservices**] [**extend**]

no ip fastnat

参数

参数	参数说明
outside *interface-type number*	指定的标记为NAT OUTSIDE的网络接口，该网络接口是主线路的出口。
backup-outside *interface-type number*	[可选]指定的标记为NAT OUTSIDE的网络接口，该网络接口是备份线路的出口。
inside interface type number	指定的标记为NAT INSIDE的网络接口，该网络接口是备份线路的入口。
privateservices	[可选]开启私服功能
extend	[可选]开启支持扩展访问列表功能

缺省

无

命令模式

全局配置态

使用说明

该命令的使用对网络环境有限制，具体信息请参考配置说明书。

如果不使用私服或者扩展访问列表，则建议不要配置选项 **privateservices** 和 **extend**。

2.1.5 ip nat inside destination

用 ip nat inside destination 全局配置命令，开启内部目的地址的 NAT.用这个命令的 NO 形式，删除和地址池的动态关联，注意，该规则正在使用时，不能删除。

ip nat inside destination list *access-list-name* **pool** *name*

no ip nat inside destination list *access-list-name*

参数

参数	参数说明
list name	标准IP访问列表的名字。用来自被指定的池中的全局地址对带有目的地址的报文进行翻译，这些包用来发送访问列表。
pool name	地址池的名字，在动态翻译的过程中，从这个池中分配内部本地的IP地址。

缺省

内部目的地址不被翻译。

命令模式

全局配置态

使用说明

这个命令用访问列表的格式来建立动态地址翻译。来自和标准访问列表相匹配的地址的报文，将用指定的地址池中分配的全局地址来进行地址翻译，这个地址池是用 ip nat pool 命令所指定的。

示例

下面的例子把发往 171.69.233.208 网络通信的报文翻译为目的地址位于 192.168.2.208 网段的内部主机地址。

```
ip nat pool net-208 192.168.2.208 192.168.2.223 255.255.255.240
ip nat inside destination list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standar a1
 permit 171.69.233.208 255.255.255.240
!
```

2.1.6 ip nat inside source

使用 ip nat inside source 全局配置命令，开启内部源地址的 NAT。用这个命令的 NO 形式可以删除静态翻译或删除和池的动态关联，注意：动态翻译规则和静态网段翻译规则在使用时，不能删除。

动态 NAT：

ip nat inside source {**list** *access-list-name*} {{**interface** *type number* | **pool** *pool-name*} [**overload**]} | {**interface** *type number* **fixed-srcport** *begin-ipaddress end-ipaddress base-port total-ports***}**

no ip nat inside source {**list** *access-list-name*} {{**interface** *type number* | **pool** *pool-name*} [**overload**]} | {**interface** *type number* **fixed-srcport** *begin-ipaddress end-ipaddress base-port total-ports***}**

静态单个地址 NAT：

ip nat inside source {**static** {*local-ip global-ip*}

no ip nat inside source {**static** {*local-ip global-ip*}

静态端口 NAT：

ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port* {*global-ip* | **interface** *type number*} *global-port*}

no ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port* {*global-ip* | **interface** *type number*} *global-port*}

静态网段 NAT：

ip nat inside source {**static** {**network local-network global-network** *mask*}

no ip nat inside source {**static** {**network local-network global-network** *mask*}

参数

参数	参数说明
List access-list-name	IP访问列表的名字。源地址符合访问列表的报文将被用地址池中的全局地址来翻译。
pool name	地址池的名字，从这个池中动态地分配全局IP地址。
interface type number	指定网络接口
overload	（可选）使路由器对多个本地地址使用一个全局的地址。当OVERLOAD被设置后，相同或者不同主机的多个会话将用TCP或UDP端口号来区分。
static local-ip	建立一条独立的静态地址翻译；参数为分配给内部网主机的本地IP地址。这个地址可以自由的选择，或从RFC 1918中分配。
local-port	设置本地TCP/UDP端口号，范围为1～65535。
static global-ip	建立一条独立的静态地址翻译；这个参数为内部主机建立一个外部的网络可以唯一访问的IP地址。
global-port	设置全局TCP/UDP端口号，范围为1～65535。
tcp	设置TCP端口翻译
udp	设置UDP端口翻译
network local-network	设置本地网段翻译
global-network	设置全局网段翻译
mask	设置网段翻译的网络掩码

缺省

任何内部源地址的 NAT 都不存在。

命令模式

全局配置态

使用说明

这个命令有两种形式：动态的和静态的地址翻译。带有访问列表的格式建立动态翻译。来自和标准访问列表相匹配的地址的报文，将用指定的池中分配的全局地址来进行地址翻译，这个池是用 ip nat pool 命令所指定的。

可以作为替代方法，带有关键字 STATIC 的语法格式创建一条独立的静态地址翻译。

静态 NAT 对于 FTP 的 PASV 模式的支持需要配合 overload 类型的命令使用，既：当设置一个 NAT 的静态 FTP 映射时，如果也需要使用 FTP 的 PASV 模式，也应该同时使用一个 overload 类型的转换，且 pat 规则中的外网接口地址中应该有一个和静态 ftp 的外网地址相同。

示例

下面的例子把来自 192.168.1.0 或 192.168.2.0 网络的内部主机间进行通信的 IP 地址翻译为 171.69.233.208/28 网络中全局唯一的 IP 地址。

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
 permit 192.168.2.0 255.255.255.0
!
```

静态 FTP 的 PASV 模式使用示例。

```
ip nat inside source static tcp 10.1.1.1 21 204.112.1.2 8021
ip nat inside source static tcp 10.1.1.1 20 204.112.1.2 8020
ip nat inside source list test1 interface f0/0
```

2.1.7 ip nat outside source

使用 ip nat outside source 全局配置命令，开启外部源地址的 NAT。用这个命令的 NO 形式，可以删除静态条目或动态关联，注意：动态翻译规则和静态网段翻译规则在使用时，不能删除。

动态 NAT

ip nat outside source {**list** *access-list-name*} **pool** *pool-name*

no ip nat outside source {**list** *access-list-name*} **pool** *pool-name*

静态单个地址 NAT：

ip nat outside source static {*global-ip local-ip*}

no ip nat outside source static {*global-ip local-ip*}

静态端口 NAT：

ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*}

no ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*}

静态网段 NAT：

ip nat outside source {**static network** *global-network local-network mask*}

no ip nat outside source {**static network** *global-network local-network mask*}

参数

参数	参数说明
List access-list-name	标准IP访问列表的名字。目的地址符合访问列表的报文将被用地址池中的全局地址来翻译。。
pool name	池的名字，从这个池重动态地分配全局IP地址。
Static global-ip	建立一条独立的静态地址翻译；参数为建立外部网络的主机所分配的全局IP地址。这个地址可以从全局可路由的网络地址空间中分配。
global-port	设置全局TCP/UDP端口号，范围为1～65535。
Static local-ip	建立一条独立的静态地址翻译；这个参数为内部主机建立一个内部网络可以唯一访问的外部主机的本地IP地址。这个地址可以从内部网络可路由的地址空间中分配。（多遵从RFC 1918）
local-port	设置本地TCP/UDP端口号，范围为1～65535。
tcp	设置TCP端口翻译
udp	设置UDP端口翻译
network global-network	设置全局网段翻译
local-network	设置本地网段翻译
mask	设置网段翻译的网络掩码

缺省

不存在来自外部网络的源地址到内部网络地址的翻译。

命令模式

全局配置态

使用说明

可能你用了不是合法的、正式分配得到的 IP 地址。可能你选择了已经被正式分配给其他网络的 IP 地址。这种 IP 地址既被合法的使用了（外部网）又被非法的使用着（内部网络）的情况叫做“地址重叠”（*overlapping*）。你可以用 NAT 来翻译和外部地址重叠的内部地址。如果你的单连接网络中的 IP 地址碰巧和分配给其他网络的合法 IP 地址相同，并且你需要和这些主机或路由器通信，那么你可以用这个功能。

这个命令有两种形式：动态的和静态的地址翻译。带有访问列表的格式建立动态地址翻译。来自和标准访问列表相匹配的地址的报文，将用指定的地址池中分配的本地地址来进行地址翻译，这个地址池是用 ip nat pool 命令所指定的。

作为可以替代的方法，带有关键字 STATIC 的语法格式创建一条单独的静态翻译。

示例

下面的例子把来自 9.114.11.0 网络的内部主机间进行通信的 IP 地址翻译为 171.69.233.208/28 网络中全局唯一的 IP 地址。更进一步地，来自 9.114.11.0 网络（真实存在的 9.114.11.0 网络）编址的外部主机的报文，被翻译为以来自 10.0.1.0/24 网络的面目出现。

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
ip nat inside source list a1 pool net-208
ip nat outside source list a1 pool net-10
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 9.114.11.39 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 9.114.11.0 255.255.255.0
!
```

2.1.8 ip nat pool

用 ip nat pool 全局配置命令，定义一个用于 NAT 的 IP 地址池。用这个命令的 NO 形式，可以删除指定名字的 IP 地址池，可以配置相同名字的地址池来覆盖已配置的地址池

ip nat pool name *start-ip end-ip netmask* [**rotary**]

no ip nat pool *name*

参数

参数	参数说明
name	池的名字。
start-ip	定义IP地址池的范围：起始地址。
end-ip	定义IP地址池的范围：结束地址。
netmask	子网掩码。子网掩码表明地址中的那些位是属于网络和子网部分，而哪些位属于主机部分。指定IP池中地址所属的网络的子网掩码。
rotary	轮循地址池 。

缺省

没有定义 IP 池。

命令模式

全局配置态

使用说明

这个命令用起始地址，结束地址以及子网掩码来定义一个地址池。注意,在 PAT 规则下,地址池的轮循规则:只有当一个地址使用完结时(即关于这个地址的所有连接都老化后),才去取下一个地址,即同一使用时间内,内部全局地址始终只有一个。

示例

下面的例子把来自 192.168.1.0 或 192.168.2.0 网络的内部主机间进行通信的 IP 地址翻译为 171.69.233.208/28 网络中全局唯一的 IP 地址。

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
 permit 192.168.2.0 255.255.255.0
```

2.1.9 ip nat service

此命令是为 Nat 支持的各种服务提供的一个入口函数，目前支持三类的服务。缺省各种服务都为关闭状态。

ip nat service { **h323** | **privateservice** | **peek** }

no ip nat service { **h323** | **privateservice** | **peek** }

参数

无

缺省

关闭

命令模式

全局配置态

使用说明

h323 对 voip 的支持，它用来控制 Nat 对 h323 的支持；

privateservice 是 Nat 对网吧设置内部游戏服务器的支持，如：传奇等；它可以控制 Nat 对于私服的支持；

peek 是 Nat 对网吧内部监控游戏服务器的支持，通过搭配公司的客户端软家，可以对内部用户出网的情况进行监控。

no 方式可以关闭相应的功能；

示例

ip nat service privateservice
ip nat service peek
ip nat service h323
no ip nat service peek

2.1.10 ip nat translation

ip nat translation 全局配置命令，主要有以下两种用途：

其一，改变 NAT 翻译超时的时间值，用这个命令的 NO 形式，可以关闭超时。

ip nat translation {timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | syn-timeout } *seconds*

no ip nat translation {timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | syn-timeout }

其二，改变针对 NAT 翻译表项的一些参数值，用此命令的 NO 形式，可以去掉配置，有默认值的恢复默认值。

ip nat translation max-entries { **host** [*A.B.C.D* | **any**] } *numbers*

no ip nat translation max-entries { **host** [*A.B.C.D* | **any**] }

参数

参数	参数说明
timeout	指定用于除OVERLOAD翻译之外的动态翻译的超时值。缺省值是3600秒（1小时）
udp-timeout	指定用于UDP端口的超时值。缺省值是300秒（5分钟）
dns-timeout	指定用于连到DNS的超时值。缺省值是60秒
tcp-timeout	指定用于TCP端口的超时值。缺省值是3600秒（1小时）
finrst-timeout	指定用于Finish and Reset TCP报文的超时值，这个值用于终止一个翻译表项。缺省值使60秒
icmp-timeout	设置ICMP的NAT超时时间,缺省值是60秒

max-entries	设置NAT的最大翻译条目数,缺省值是3000
syn-timeout	设置TCP SYN状态的NAT超时时间,缺省值是60秒
seconds	指定端口翻译的超时值。缺省值是在缺省部分所罗列出来的值
max-entries host *A.B.C.D*	针对指定的内部IP地址，限制该IP地址能建立NAT翻译表项的最大数目，无缺省值，当用该命令的no形式时，即不在限制该IP地址建立NAT翻译表项的数目
max-entries host any	针对所有的内部IP地址，限制单个IP地址能建立NAT翻译表项的最大数目。缺省值与max-entries相同

缺省

timeout is 3600 seconds (1 hours)

udp-timeout is 300 seconds (5 minutes)

dns-timeout is 60 seconds (1 minute)

tcp-timeout is 3600 seconds (1 hours)

finrst-timeout is 60 seconds (1 minute)

命令模式

全局配置态

使用说明

当配置了端口翻译之后，因为每个翻译条目包含了有关正在使用它的通信量更多的上下文信息，因此可以对翻译条目进行更好的控制。非域名系统（DNS）的 UDP 翻译在 5 分钟后超时，而域名系统的 UDP 翻译在 1 分钟后超时。如果数据流中没有 RST 或 FIN，TCP 翻译在 1 个小时后超时；而在有 RST 或 FIN 的情况下，将在 1 分钟后超时。

示例

例 1：

下面的例子在 10 分钟之后使 UDP 端口翻译条目超时：

ip nat translation udp-timeout 600

例 2：

下面的例子限制 IP 地址 192.168.20.1 建立的 NAT 翻译表项的最大数目为 100：

ip nat translation max-entries host 192.168.20.1 100

2.1.11 ip nat log

ip nat log 全局配置命令，主要有以下两种用途：

其一，打开 nat 条目的 syslog 记录。

ip nat log translations syslog

其二，改变针对 NAT 翻译表项的一些参数值，用此命令的 NO 形式，可以去掉配置，有默认值的恢复默认值。

ip nat log event syslog

参数

无

缺省

无

命令模式

全局配置态

使用说明

当配置了端口翻译之后，为了记录 nat 的日志，可以使用 log 命令。

使用之后，对性能会有少许影响。

示例

下列命令开启 nat 条目相关日志：

ip nat log translations syslog

下列命令开启 nat 状态相关日志：

ip nat log event syslog

2.1.12 ip nat translation max-users[不再支持]

配置 nat 限制上网用户数的功能。

[**no**] **ip nat translation max-users** <0-65536>

[**no**] **ip nat translation max-users enable**

参数

参数	参数说明
0-65536	设置可以上网的内网用户数，缺省为256个。

缺省

缺省内网的用户数为 256 个，缺省不开启这个功能。

命令模式

全局配置态。

使用说明

通过这个命令可以开启和设置 nat 限制内网用户数的功能。当一个用户上网时，如果之前在 NAT 中没有对应的记录，那么他就是一个新内网用户。如果这时内网用户上网数量已经达到设定值，那么这个用户发向外面的报文将被抛弃，该用户将不可以上网。如果内网用户数量没有达到限制值，NAT 就记录该用的 IP 地址，并进行正常的报文转发过程。

所记录用户 IP 地址的超时时间与该用户的最后一次发送的报文所属的 link 的 ttl 值相同。

NO 方式关闭该功能。

示例

下列命令在全局态配置 nat 的限制功能：

```
ip nat translation max-users enable
ip nat translation max-users 124
```

2.1.13 clear ip nat statistics

为了清除 NAT 的统计信息，使用 clear ip nat statistics 命令。

clear ip nat statistics

参数

无

命令模式

管理态

使用说明

使用本命令可以把所有 NAT 统计信息置为初始状态。

注意：

只能清楚“Packets dropped”项后面的统计参数。

示例

```
Router#show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
   FastEthernet0/1
Inside interfaces:
   FastEthernet0/0
Dynamic mappings:
--Inside Source
      access-list nat
      pool natp: netmask 255.255.255.0
      start 172.16.20.125   end 172.16.20.127
      total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
   PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6
```

```
Packets dropped:
--Protocol:
    Out: tcp 123, udp 39, icmp 10, others 6
    In: tcp 46, udp 109, icmp 0, others 10
--Configuration:
    max entries 0, max entries for host 178
Router#clear ip nat statistics
Router#show ip nat statistic
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
    FastEthernet0/1
Inside interfaces:
    FastEthernet0/0
Dynamic mappings:
--Inside Source
      access-list nat
      pool natp: netmask 255.255.255.0
      start 172.16.20.125    end 172.16.20.127
      total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
    PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6
Packets dropped:
--Protocol:
    Out: tcp 0, udp 0, icmp 0, others 0
    In: tcp 0, udp 0, icmp 0, fragments 0
--Configuration:
    max entries 0, max links for host 0
```

2.1.14 clear ip nat translation

为了从翻译表项中清除动态网络地址翻译（NAT），使用 **clear ip nat translation** 执行命令。

clear ip nat **translation** {***** | [**inside** local-ip global-ip] [**outside** local-ip global-ip]}

clear ip nat translation {**tcp|udp**} **inside** *local-ip local-port global-ip global-port* [**outside** *local-ip global-ip*]

参数

参数	参数说明
*	清除所有的动态翻译条目
Inside	清除包含指定全局IP地址和本地IP地址的内部翻译。
global-ip	指定全局IP地址
local-ip	指定本地IP地址
outside	清除包含指定全局IP地址和本地IP地址的外部翻译。
tcp|udp	协议
global-port	指定相应协议的全局端口。
local-port	指定相应协议的本地端口。

命令模式

管理态

使用说明

使用本命令可以在动态翻译条目超时之前清除他们。

示例

下面的例子先显示 NAT 翻译条目，然后将 UDP 翻译条目清除：

```
Router# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53     171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23   171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23     171.69.1.161:23
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
Router# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23   171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23     171.69.1.161:23
```

2.1.15 show ip nat statistics

用 show ip nat statistics 命令，显示 NAT 统计表

show ip nat statistics

参数

这个命令没有参数或关键字

命令模式

管理态

示例

下面是使用 show ip nat statistics 命令的例子的输出结果：

```
Router# show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
   FastEthernet0/1
Inside interfaces:
   FastEthernet0/0
Dynamic mappings:
--Inside Source
      access-list nat
      pool natp: netmask 255.255.255.0
      start 172.16.20.125    end 172.16.20.127
      total addresses 3, misses 0
--Inside Destination
```

--Outside Source
Link items:
PAT(ICMP=0 UDP=5 TCP=24 / TOTAL=29), Dynamic=0
Packets dropped:
--Protocol:
Out: tcp 0, udp 0, icmp 0, others 0
In: tcp 46, udp 100, icmp 0, others 0
--Configuration:
max entries 0, max links for host 0

表 9 描述了输出结果中的重要字段：

表 2-1 Show ip nat statistics 字段描述

字段	描述
Total active translations:	系统中激活的指定翻译的数量。当建立了一个地址翻译规则时，这个数值将被加1，同时当一个地址翻译被清除或超时，这个数值将减1。
Outside interfaces:	用ip nat outside 命令标识为外部接口的接口列表。
Inside interfaces:	用ip nat outside 命令标识为内部接口的接口列表。
Dynamic mappings:	显示跟在它后面的信息是关于动态映射的。
Inside Source:	跟在它后面的是关于内部源地址翻译的信息.
Access-list	用于地址翻译的访问列表数量。
Pool	池的名字（本例中池的名字是natp）
Netmask	池中所使用的IP网络掩码
Start	池中地址范围的起始IP地址.
End	池中地址范围的结束IP地址.
Total addresses	池中可用于地址翻译的地址数.
Misses	无法从池中分配的地址数量.
Inside Destination:	跟在它后面的是关于内部目的地址翻译的信息.
Outside Source:	跟在它后面的是关于外部源地址翻译的信息.
Link items:	跟在它后面的是关于翻译表项数目和类别的信息.
PAT	表示动态端口翻译规则下的翻译表项数目,其中madia代表H323会话中的RTP/RTCP会话.
Dynamic	表示动态地址翻译规则下的翻译表项数目,包括静态地址翻译为FTP创建的翻译表项.
Packets dropped:	跟在它后面的是关于因为NAT而丢弃的报文的类型和数目,以及丢弃的原因.
Protocol	表示丢弃报文的数目、协议类型和报文的NAT方向.
Configuration	表示因为何种配置丢弃的报文的数目:max entries指超过最大允许

	翻译表项数,max links for host指超过每个或者特定地址允许的翻译表项数.

2.1.16 show ip nat translations

用 show ip nat translations 管理态命令，显示激活的 NAT 地址翻译。

show ip nat translations [**host** *A.B.C.D* | **tcp** | **udp** | **icmp** | **verbose**]

参数

参数	参数说明
host *A.B.C.D*	（可选）显示承载本地局部地址(inside local)为 *A.B.C.D* 的翻译表项
tcp	（可选）显示承载TCP会话的翻译表项
udp	（可选）显示承载UDP会话的翻译表项
icmp	（可选）显示承载ICMP会话的翻译表项
Verbose	（可选）显示关于每个翻译表项的额外信息，包括它被建立了多久，还剩下多长时间超时

命令模式

管理态

使用说明

示例

下面是使用 show ip nat translations 命令的例子的输出结果。

(1) 两个内部主机和外部的一些主机进行报文交换，没有超载。

```
Router# show ip nat translations
Pro Inside local      Inside global      Outside local      Outside global
--- 192.168.1.95      171.69.233.209     ---                ---
--- 192.168.1.89      171.69.233.210     ---                --
```

(2) 下面是带有超载的情况下的示例，有三条地址翻译表项是激活的，其中一条用于一个 DNS 业务，另外两条用于 TELNET 会话（来自两个不同的主机）。要注意：两个不同的内部主机能以具有相同外部地址的形式出现。

```
Router# show ip nat translations
Pro Inside local       Inside global          Outside local      Outside global
udp 192.168.1.95:1220  171.69.233.209:1220    171.69.2.132:53    171.69.2.132:53
tcp 192.168.1.89:11012 171.69.233.209:11012   171.69.1.220:23    171.69.1.220:23
tcp 192.168.1.95:1067  171.69.233.209:1067    171.69.1.161:23    171.69.1.161:23
```

下面是带有关键字 verbose 的输出样例：

```
Router# show ip nat translations verbose
Pro Inside local      Inside global      Outside local      Outside global
udp 192.168.1.95:1220 171.69.233.209:1220 171.69.2.132:53    171.69.2.132:53
```

create time 00:00:02 , left time 00:01:10 ,
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23 171.69.1.220:23
create time 00:01:13 , left time 00:00:50 ,
tcp 192.168.1.95:1067 171.69.233.209:1067 171.69.1.161:23 171.69.1.161:23
create time 00:00:02 , left time 00:53:19 ,

表 2-2 Show IP NAT Translations（例 2）命令输出结果的字段描述

字段	描述
Pro	确定地址的端口协议.
Inside global	合法的IP地址（被NIC或服务提供商所提供的），他们代表了通往外部网络的一个或多个内部本地IP地址。
Inside local	被分配给内部网络中主机的IP地址；他们可能不是一个NIC或服务供应商所提供的合法地址。
Outside local	一个外部主机当它看起来像是一个内部网络时的IP地址；他们可能不是一个NIC或服务供应商所提供的合法地址。
Outside global	被它的所有者所分配的外部主机的IP地址。
Create time	地址翻译条目是多久前建立的。（单位是 小时：分：秒）
Left time	地址翻译条目经过多久会超时。

2.1.17 show ip nat users[不再支持]

显示当前允许通过的内网用户 IP 地址，以及数量。

show ip nat users

参数

无

缺省

无

命令模式

全局配置态。

使用说明

显示当前允许通过的内网用户 IP 地址，以及数量。

由于这个功能需要进行一定量的操作步骤，如果不是很必要，请不要开启这个功能。

示例

下列命令在全局态执行：

show ip nat users

一个可能的显示结果如下：

```
                    Current host count is 9, host count set is 12.
 #host IP   addr   host ttl
 172.16.20.67        20
 172.16.20.70        55
 172.16.20.81        3530
 172.16.20.90        3600
```

2.1.18 debug ip nat

为了调试网络地址翻译（NAT），使用 **debug ip nat** 执行命令。

debug ip nat {**detail** | **h323**}

no debug ip nat {**detail** | **h323**}

参数

无

命令模式

管理态

使用说明

使用命令 **debug ip nat detail** 可以输出翻译过程中的细节，包括报文的源、目的 IP 地址，协议、端口号，以及没有成功的翻译的原因等等。

使用命令 **debug ip nat h323** 可以输出 NAT 在翻译 H323 报文过程中的细节，主要包括 NAT 识别出的 H323 消息，以及嵌入在这些消息里的 IP 地址，如果是内部地址，将会显示翻译后的地址。

示例

例 1 ：

```
Router# debug ip nat detail
Ethernet1/1 recv ICMP Src 194.4.4.89 Dst 10.10.10.102 no link found
Ethernet1/0 send TCP Src 194.4.4.102:2000 Dst 192.2.2.1:21 no matched rule
```

表 2-3 表描述了显示中的域。

域	描述
Ethernet1/0	接口的类型、号。
send/recv	发送/接收。
ICMP/TCP/UDP	ICMP/TCP/UDP协议
Src 194.4.4.102:2000	源IP地址和端口号。
Dst 192.2.2.1:21	目的IP地址和端口号。
no link found	没有匹配到NAT翻译表项。
no matched rule	没有匹配到NAT规则。

第 1 条：从 Ethernet1/1 接口接收到的 ICMP 报文（源地址是 194.4.4.89，目的地址是 10.10.10.102；ICMP），没有找到相应的 NAT 翻译表项（已经找到匹配的 NAT 规则）。

第 2 条：从 Ethernet1/0 接口发送出去的 TCP 报文（源地址是 194.4.4.102，目的地址是 192.2.2.1；源端口是 2000，目的端口是 21），没有找到匹配的 NAT 规则。

例 2：

```
Router# debug ip nat h323
NAT:H225:[I] processing a Setup message
NAT:H225:[I] found Setup sourceCallSignalling
NAT:H225:[I] fix TransportAddress addr-192.168.122.50:11140
NAT:H225:[I] found Setup fastStart
NAT:H225:[I] Setup fastStart PDU length:18
NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1
NAT:H245:[I] found OLC forward mediaControlChannel
NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16517
NAT:H225:[I] Setup fastStart PDU length:29
NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1
NAT:H245:[I] found OLC reverse mediaChannel
NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16516
NAT:H245:[I] found OLC reverse mediaControlChannel
NAT:H245:[O] fix TransportAddress addr-192.168.122.50:16517
NAT:H225:[O] processing an Alerting message
NAT:H225:[O] found Alerting fastStart
NAT:H225:[O] Alerting fastStart PDU length:25
NAT:H245:[O] processing OpenLogicalChannel message, forward channel 1
```

重要域的描述见下表：

域	描述
NAT	表示报文已经被NAT翻译
RAS/H255/H245	报文协议类型
O	表示报文的传输方向：Inside to Outside
I	表示报文的传输方向：Outside to Inside

ip nat service firewall

ip nat service firewall {i2o | o2i}

no ip nat service firewall {i2o | o2i}

参数

参数	参数说明
I2o	打开 inside 端口到 outside 端口的 NAT 防火墙
O21	打开 outside 端口到 inside 端口的 NAT 防火墙 缺省

无

命令模式

全局配置态

使用说明

虽然名为防火墙，但工作原理跟防火墙有很大的不同，其本质是让路由器只运行 NAT 这个 IP 进程，其余的 IP 服务（如 IPSEC，VPN 等）就不再处理了。i2o 就是数据包从 inside 到 outside 时，如果不符合 NAT，就直接丢弃，不再检查其是否有其他的 IP 服务了；o2i 是从 outside 到 inside 时，如果找不到 nat cache 时，则数据包直接丢弃，不再进行其他检查了。

注意：

这两个 firewall 的功能是用于简化路由器的处理流程，一方面可以提高 NAT 的效率，但另一方面也会导致某些功能的实效。

第3章 DHCP Client 配置命令

3.1 DHCP Client配置命令

DHCP Client 配置命令包括：

- ip address dhcp
- ip dhcp client
- ip dhcp-server
- show dhcp lease
- show dhcp server
- debug dhcp

3.1.1 ip address dhcp

要通过 Dynamic Host Configuration Protocol（DHCP）为以太网接口获得一个 IP 地址，使用 ip address dhcp 接口配置命令。要删除所获得的 IP 地址，可以使用这条命令的 no 格式。

ip address dhcp

no ip address dhcp

参数

无

缺省

无

命令模式

接口配置态

使用说明

ip address dhcp 命令允许接口通过 DHCP 协议获得 IP 地址，这对通过以太网接口动态连接 Internet 服务提供商（ISP）非常有用。一旦获得了动态的 IP 地址，这个以太网接口便可以使用端口转换技术（PAT）来实现网络地址翻译（NAT）。

如果路由器上配置了 ip address dhcp 命令，路由器将向网络上的 DHCP 服务器发送 DHCPDISCOVER 消息。

如果路由器上配置了 no ip address dhcp 命令，路由器将发送 DHCP RELEASE 消息。

示例

以下例子使得 Ethernet1/1 接口通过 DHCP 协议来获得接口的 IP 地址。

!

```
interface Ethernet1/1
 ip address dhcp
```

相关命令

ip dhcp client

ip dhcp-server

show dhcp lease

show dhcp server

3.1.2 ip dhcp client

配置本地路由器 DHCP 客户端的参数。

ip dhcp client { **minlease seconds | retransmit count | select seconds** }

no ip dhcp client { **minlease | retransmit | select** }

参数

参数	参数说明
minlease seconds	（可选）可接受的最小租用时间，范围从60～86400秒。
retransmit count	（可选）协议报文的重传次数，范围从1～10。
select seconds	（可选）SELECT的时间间隔，范围从0～30。

缺省

minlease 参数缺省值为 60 秒。

retransmit 参数缺省值为 4 次。

select 参数缺省值为 0 秒。

命令模式

全局配置态。

使用说明

根据网络结构和 DHCP 服务器的需要，来调整这些参数。

如果配置了这些命令的 no 格式命令，则这些参数恢复成系统定义的缺省值。

示例

以下例子设置了路由器上 DHCP 客户端可接受的最小租用时间为 100 秒。

```
ip dhcp client minlease 100
```

以下例子设置了路由器上 DHCP 客户端协议报文重传次数为 3 次。

```
ip dhcp client retransmit 3
```

以下例子设置了路由器上 DHCP 客户端 SELECT 的时间间隔为 10 秒。

ip dhcp client select 10

相关命令

ip address dhcp

ip dhcp-server

show dhcp lease

show dhcp server

3.1.3 ip dhcp-server

要指定已知的 DHCP 服务器，可以使用 ip dhcp-server 命令来指定 DHCP 服务器的 IP 地址。

ip dhcp-server *ip-address*

no ip dhcp-server *ip-address*

参数

参数	参数说明
ip-address	DHCP服务器的IP地址。

缺省

无任何缺省的 DHCP 服务器 IP 地址。

命令模式

全局配置态。

使用说明

使用此命令可以指定一个 DHCP 服务器的 IP 地址，该命令不会覆盖以前指定的 DHCP 服务器 IP 地址。

使用此命令的 no 格式命令可以用来清除以前配置的 DHCP 服务器 IP 地址。

示例

下面的例子显示了在路由器上如何指定 IP 地址为 192.168.20.1 的服务器为 DHCP 服务器：

ip dhcp-server 192.168.20.1

相关命令

ip address dhcp

ip dhcp client

show dhcp lease

show dhcp server

3.1.4 show dhcp lease

要查看当前路由器所使用的 DHCP 服务器分配的信息，可以用 show dhcp lease 命令来实现。

Show dhcp lease

参数

无

缺省

无

命令模式

管理态

使用说明

使用此命令可以查看当前路由器所使用的 DHCP 服务器分配的信息。

示例

下面的例子显示了路由器所使用 DHCP 分配的信息：

```
router#show dhcp lease
Temp IP addr: 192.168.20.3    for peer on Interface: Ethernet1/1
Temp    sub net mask: 255.255.255.0
    DHCP Lease server: 192.168.1.3, state: 4 Rebinding
    DHCP transaction id: 2049
    Lease: 86400 secs,    Renewal: 43200 secs,    Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.2
    Next timer fires after: 02:34:26
    Retry count: 1     Client-ID: router-0030.80bb.e4c0-Et1/1
```

相关命令

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp server

debug dhcp

3.1.5 show dhcp server

要显示已知的 DHCP 服务器信息，可以使用 show dhcp server 命令来实现。

show dhcp server

参数

无

缺省

无

命令模式

管理态

使用说明

使用此命令可以显示已知的 DHCP 服务器信息。

示例

下面的例子已知的 DHCP 服务器信息。

```
router#show dhcp sever
DHCP server: 255.255.255.255
  Leases:   0
  Discovers: 62 Requests: 0      Declines: 0      Releases: 0
  Offers:     0   Acks:      0      Naks:      0      Bad:       0
  Subnet: 0.0.0.0,        Domain name:
```

相关命令

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp lease

3.1.6 debug dhcp

当路由器上 dhcp 运行时，要查看 dhcp 协议的处理状况，可以运行 debug dhcp 命令。

debug dhcp <detail>

no debug dhcp <detail>

参数

参数	参数说明
detail	显示DHCP协议报文内容。

缺省

缺省情况下不显示相关信息。

命令模式

管理态

使用说明

显示和 DHCP 处理相关的一些重要处理信息，举例如下：

```
router#debug dhcp
router#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7
2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet
2000-4-22 10:50:40 DHCP:          B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:40 DHCP: Move to SELECTING state, xid: 0x7
2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket
2000-4-22 10:50:46 DHCP:          B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:54 DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket
```

相关命令

show dhcp lease

第4章 DHCP Sever 配置命令

4.1 DHCPD配置命令

DHCPD 配置命令包括：

- ip dhcpd ping packet
- ip dhcpd ping timeout
- ip dhcpd write-time
- ip dhcpd pool
- ip dhcpd enable
- ip dhcpd disable

4.1.1 ip dhcpd ping packet

ip dhcpd ping packet *pkgs*

参数

参数	参数说明
pkgs	DHCP服务器用于检测地址是否已经分配所发送的ICMP包个数。

缺省

2

命令模式

全局配置态

使用说明

用户可以使用如下命令来配置 DHCP 服务器在检查地址是否已经分配时，发送 n 个 ICMP 包。

ip dhcpd ping packets n

示例

以下命令配置 DHCP 服务器在检查地址是否已经分配时，发送 1 个 ICMP 包。

ip dhcpd ping packets 1

4.1.2 ip dhcpd ping timeout

参数

参数	参数说明

timeout	DHCP服务器用于检测地址是否已经分配时，等待ICMP包响应的超时时间（以100毫秒为单位）。

缺省

5

命令模式

全局配置态

使用说明

用户可以使用如下命令来配置 DHCP 服务器在检查地址是否已经分配时，等待 ICMP 包响应的超时时间为 n*100ms。

ip dhcpd ping timeout n

示例

以下命令配置 DHCP 服务器在检查地址是否已经分配时，等待 ICMP 包响应的超时时间为 300ms。

ip dhcpd ping timeout 3

4.1.3 ip dhcpd write-time

参数

参数	参数说明
time	DHCP服务器将地址分配信息保存到数据库中的间隔时间（以分钟为单位）。

缺省

60

命令模式

全局配置态

使用说明

用户可以使用如下命令来配置 DHCP 服务器每隔 n 分钟，就将地址分配信息写入数据库中

ip dhcpd write-time n

建议用户不要将此值设置得比缺省值小 。

示例

以下命令配置 DHCP 服务器每隔 1 天将就将地址分配信息写入数据库中

ip dhcpd write-time 1440

4.1.4 ip dhcpd pool

参数

参数	参数说明
name	DHCP地址池的名称。

缺省

无

命令模式

全局配置态

使用说明

用户可以使用如下命令来增加名为 name 的 DHCP 地址池，并进入 DHCP 地址池配置模式

ip dhcpd pool name

示例

以下命令增加名为 test 的 DHCP 地址池，同时进入 DHCP 地址池配置模式。

ip dhcpd pool test

4.1.5 ip dhcpd enable

参数

无

缺省

缺省情况下，关闭 DHCP 服务

命令模式

全局配置态

使用说明

用户可以使用如下命令来打开 DHCP 服务。 此时，DHCP 服务器也支持 relay 操作，对于自身不能分配的地址请求，配置了 ip helper-address 的端口将转发 DHCP 请求。

ip dhcpd pool name

示例

以下命令打开 DHCP 服务。

ip dhcpd enable

4.1.6 ip dhcpd disable

参数

无

缺省

无

命令模式

全局配置态

使用说明

用户可以使用如下命令来关闭 DHCP 服务

ip dhcpd disable

示例

以下命令关闭 DHCP 服务。

ip dhcpd disable

4.2 DHCPD地址池的配置命令

DHCPD 地址池的配置命令包括：

- network
- range
- default-router
- dns-server
- domain-name
- lease
- netbios-name-server
- host
- hardware-address
- client-identifier
- client-name

4.2.1 network

network *ip-addr netmask*

参数

参数	参数说明
ip-addr	用于自动分配的地址池的网络地址。
netmask	子网掩码。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置用于自动分配的地址池的网络地址。此命令只用于自动分配方式。

在配置该命令时，务必确保接收 DHCP 协议报文的端口上有一个端口 IP 地址的网络号和 network 相同。

示例

以下命令配置 DHCP 地址池的网络地址为 192.168.20.0，子网掩码为 255.255.255.0。

network 192.168.20.0 255.255.255.0

4.2.2 range

range *low-addr high-addr*

参数

参数	参数说明
low-addr	用于自动分配地址区域的起始地址。
hogh-addr	用于自动分配地址区域的终止地址。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置用于自动分配的地址区域。每个地址池最多可配置 8 个 range，每个 range 均必须在 network 范围内。此命令只用于自动分配方式，

示例

以下命令配置 DHCP 地址池的地址分配区域为 192.168.20.210－192.168.20.219。

range 192.168.20.210 192.168.20.219

4.2.3 default-router

default-router *ip-addr*

参数

参数	参数说明
ip-addr	分配给客户机的缺省路由。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置分配给客户机的缺省路由，最多可配置 4 个缺省路由，中间用空格分隔

示例

以下命令配置分配给 DHCP 客户机的缺省路由为 192.168.20.1。

default-router 192.168.20.1

4.2.4 dns-server

dns-server *ip-addr* …

参数

参数	参数说明
ip-addr	分配给客户机的DNS服务器地址。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置分配给客户机的 DNS 服务器地址，最多可配置 4 个 DNS 服务器，中间用空格分隔

示例

以下命令配置分配给客户机的 DNS 服务器地址为 192.168.1.3

dns-server 192.168.1.3

4.2.5 domain-name

domain-name *name*

参数

参数	参数说明
name	分配给客户机的域名。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置分配给客户机的域名

示例

以下命令配置分配给客户机的域名为 test.domain

domain-name test.domain

4.2.6 lease

lease {**days** [*hours*][*minutes*] | **infinite**}

参数

参数	参数说明
days	地址分配的天数。
hours	地址分配的小时数。

minutes	地址分配的分钟数。
infinite	地址永久分配。

缺省

1 天

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置分配给客户机的地址的时间期限。

示例

以下命令配置分配客户机的地址的时间期限为 2 天 12 小时。

Lease 2 12

4.2.7 netbios-name-server

netbios-name-server *ip-addr*

参数

参数	参数说明
ip-addr	分配客户机的netbios名字服务器地址。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置分配给客户机的 netbios 名字服务器地址，最多可配置 4 个 netbios 名字服务器，中间用空格分隔。

示例

以下命令配置分配给客户机的 netbios 名字服务器地址为 192.168.1.10

netbios-name-server 192.168.1.10

4.2.8 host

host *ip-addr netmask*

参数

参数	参数说明
ip-addr	用于手动分配的地址池的主机地址
netmask	子网掩码

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置用于手动分配的地址池的主机地址。此命令只用于手动分配方式，不能在同一个地址池中同时配置 host 和 range。

示例

以下命令配置 DHCP 地址池的手动分配地址为 192.168.20.200，子网掩码为 255.255.255.0。

host 192.168.20.200 255.255.255.0

4.2.9 hardware-address

hardware-address *hardware-address*{ **type**}

参数

参数	参数说明
hardware-address	用于匹配客户机的硬件地址。
type	硬件地址类型。

缺省

type 缺省值为 1 ，表示以太网

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置用于匹配客户机的硬件地址，地址格式为冒号分隔的两位 16 进制数 ab:cd:ef:gh。此命令只用于手动分配方式

示例

以下命令配置 DHCP 手动分配地址池的硬件地址为 10:a0:0c:13:64:7d

hardware-address 10:a0:0c:13:64:7d

4.2.10 client-identifier

client-identifier *unique-identifier*

参数

参数	参数说明
unique-identifier	用于匹配客户机的客户端ID。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置用于匹配客户机的客户端 ID，格式为点分两位 16 进制数 ab.cd.ef.gh。此命令只用于手动分配方式。

示例

以下命令配置 DHCP 手动分配地址池的客户端 ID 为 01:10:a0:0c:13:64:7d

client-identifier 01.10.a0.0c.13.64.7d

4.2.11 client-name

client-name *name*

参数

参数	参数说明
name	分配给客户机的名称。

缺省

无

命令模式

DHCP 地址池配置模式

使用说明

用户可以使用此命令来配置用于手动分配给客户机的主机名。此命令只用于手动分配方式 。

示例

以下命令配置分配给客户机的主机名为 test。

client-name test

4.3 DHCPD的调试命令

DHCPD 的调试命令包括：

- debug ip dhcpd packet
- debug ip dhcpd event

4.3.1 debug ip dhcpd packet

debug ip dhcpd packet

参数

无

缺省

无

命令模式

管理态

使用说明

用户可以使用此命令来打开 DHCPD 数据包信息的 debug 开关。

示例

以下命令打开对 DHCPD 数据包的调试信息输出开关。

debug ip dhcpd packet

4.3.2 debug ip dhcpd event

debug ip dhcpd event

参数

无

缺省

无

命令模式

管理态

使用说明

用户可以使用此命令来打开 DHCPD 事件信息的 debug 开关。

示例

以下命令打开对 DHCPD 事件的调试信息输出开关。

debug ip dhcpd event

4.4 DHCPD的管理命令

DHCPD 的管理命令包括：

- show ip dhcpd statistic
- show ip dhcpd binding
- clear ip dhcpd statistic
- clear ip dhcpd binding

4.4.1 show ip dhcpd statistic

参数

无

缺省

无

命令模式

除了用户态以外的其它状态

使用说明

用户可以使用此命令来显示 DHCPD 的统计信息，包括各类报文的数量和自动分配、手动分配的地址数

示例

以下命令显示 DHCPD 的统计信息。

Show ip dhcpd statistic

4.4.2 show ip dhcpd binding

show ip dhcpd binding {*ip-addr*}

参数

参数	参数说明
ip-addr	需要显示绑定信息的地址.

缺省

显示所有的地址绑定信息。

命令模式

除了用户态以外的其它状态

使用说明

用户可以使用此命令来显示 DHCPD 的地址绑定信息，IP 地址、硬件地址、绑定类型和超时时间

示例

以下命令显示 DHCPD 的绑定信息。

Show ip dhcpd binding

4.4.3 show ip dhcpd pool

参数

无

缺省

无

命令模式

除了用户态以外的其它状态

使用说明

用户可以使用此命令来显示 DHCPD 的地址池信息，包括地址池的网络号、地址范围、已分配地址的数目、暂时废弃的地址的数目、可以用来分配的地址数目、手动分配的 IP 地址和硬件地址。

示例

以下命令显示 DHCPD 的地址池统计信息。

show ip dhcpd pool

4.4.4 clear ip dhcpd statistic

参数

无

缺省

无

命令模式

管理态

使用说明

用户可以使用此命令来删除 DHCPD 的关于报文数量的统计信息 。

示例

以下命令删除 DHCPD 关于报文数量的统计信息。

Clear ip dhcpd statistic

4.4.5 clear ip dhcpd binding

clear ip dhcpd binding {*ip-addr*|*}

参数

参数	参数说明
ip-addr	需要删除绑定信息的地址。
*	删除所有的绑定信息。

缺省

删除指定地址绑定信息。

命令模式

管理态

使用说明

用户可以使用此命令来删除指定地址的绑定信息 。

示例

以下命令删除 192.168.20.210 的绑定信息。

clear ip dhcpd binding 192.168.20.210

以下命令删除 192.168.20.210 和 192.168.20.211 的绑定信息。

clear ip dhcpd binding 192.168.20.210 192168.20.211

以下命令删除所有的绑定信息。

clear ip dhcpd binding *

4.4.6 clear ip dhcpd abandoned

参数

无

缺省

无

命令模式

管理态

使用说明

用户可以使用此命令来清除 abandon 标志。

示例

以下命令清除 abandon 标志。

Clear ip dhcpd abandoned

第5章 DHCP-RELAY SNOOPING 配置命令

DHCP-RELAY SNOOPING 配置命令包括：

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

5.1.1 dhcp-relay snooping

命令描述

ip dhcp-relay snooping

no ip dhcp-relay snooping

配置 VLAN 的 Dhcp-relay snooping 功能开启和关闭，no 命令恢复到默认值。

参数

无

缺省

关闭 dhcp-relay snooping 功能。

说明

无。

示例

下面的命令将开启 DHCP snooping 功能：

```
Switch_config#ip dhcp-relay snooping
Switch_config#
```

5.1.2 dhcp-relay snooping vlan

命令描述

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

参数

参数	参数说明
vlan id	VLAN标识。取值范围：1-4094。

缺省

无

说明

配置 DHCP snooping 的 VLAN。

示例

下面的命令将在 VLAN 2 上对 DHCP 报文进行 snooping 检查

```
Switch_config#ip dhcp-relay snooping vlan 2
Switch_config#
```

5.1.3 dhcp-relay snooping vlan *vlan_id* max-client

命令描述

ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*

no ip dhcp-relay snooping vlan *vlan_id* **max-client**

参数

参数	参数说明
vlan id	VLAN标识。取值范围：1-4094。
number	允许最大用户数：0~65535

缺省

默认为 65536 个最大用户数。

说明

配置 DHCP snooping 的 VLAN 下的允许最大用户数，执行先到先分配的原则，当 vlan 内的用户数达到配置的允许最大值后，就不允许新的 client 进行分配。

示例

下面的命令将在 VLAN 2 上对 DHCP 报文进行 snooping 检查 ，允许最大的用户数为 3.

```
Switch_config#ip dhcp-relay snooping vlan 2 max-client 3
Switch_config#
```

5.1.4 dhcp snooping trust

命令描述

dhcp snooping trust

参数

无

缺省

默认端口为非信任端口

说明

对于 DHCP 信任端口不进行 DHCP snooping 监测，no 命令配置端口为默认值。

示例

下面的命令将端口 fastEthernet0/1 配置为 DHCP 信任端口

```
Switch_config_f0/1#dhcp snooping  trust
```

5.1.5 dhcp snooping deny

命令描述

dhcp snooping deny

参数

无

缺省

默认端口不禁止 snooping 检测

说明

关闭端口上 DHCP snooping 监测，配置之后自动打开 dhcp snooping trust、ip-source trust、arp inspection trust 。no 命令配置端口为默认值。

示例

下面的命令关闭端口 fastEthernet0/1 DHCP snooping 监测

Switch_config_f0/1#dhcp snooping deny

5.1.6 show ip dhcp-relay snooping

命令描述

show ip dhcp-relay snooping

参数

无

缺省

无

说明

显示 Dhcp-relay snooping 的配置信息。

示例

下面的命令将显示 dhcp-relay snooping 的配置信息。

Switch_config#show ip dhcp-relay snooping

5.1.7 show ip dhcp-relay snooping binding

命令描述

show ip dhcp-relay snooping binding [all]

参数

无

缺省

无

说明

显示 dhcp-relay snooping 的添加到端口绑定信息。

命令 all 显示 所有 Dhcp-relay snooping 的绑定信息

示例

下面的命令将显示 dhcp-relay snooping 的 binding 信息。

Switch_config#show ip dhcp-relay snooping binding

5.1.8 debug ip dhcp-relay snooping

命令描述

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

参数

无

缺省

无

说明

打开/关闭 Dhcp-relay snooping 的调试开关。

示例

下面的命令将打开 dhcp-relay snooping 的调试开关。

```
Switch_config#debug ip dhcp-relay snooping
Switch_config#
```

5.1.9 debug ip dhcp-relay event

命令描述

debug ip dhcp-relay eventr

no debug ip dhcp-relay event

参数

无

缺省

无

说明

打开/关闭 Dhcp-relay 的 event 调试开关。

示例

下面的命令将打开 dhcp-relay 的 event 调试开关。

```
Switch_config#debug ip dhcp-relay event
Switch_config#
```

5.1.10 debug ip dhcp-relay binding

命令描述

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

参数

无

缺省

无

说明

打开/关闭 Dhcp-relay snooping 的 binding 调试开关。

示例

下面的命令将打开 dhcp-relay snooping 的 binding 调试开关。

```
Switch_config#debug ip dhcp-relay binding
Switch_config#
```

第6章　IP 服务配置命令

6.1　IP Server配置命令

IP Server 配置命令包括：

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip rtp
- debug ip tcp packet
- debug ip tcp transactions
- debug ip udp
- ip mask-reply
- ip mtu
- ip redirects
- ip route-cache
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachables
- show ip cache
- show ip irdp
- show ip sockets
- show ip traffic
- show tcp
- show tcp brief
- show tcp statistics
- show tcp tcb

6.1.1　clear tcp

清除一个 TCP 连接。

clear tcp {*local host-name port* **remote** *host-name port* | **tcb address**}

参数

参数	参数说明
local host-name port	本地主机IP地址和TCP端口。
remote host-name port	远端主机IP地址和TCP端口。
tcb address	要清除的TCP连接的传输控制块(TCB)地址。TCB是系统内部对TCP连接的标识，可以用命令show tcp brief得到。

命令模式

管理态

使用说明

clear tcp 命令主要是用于清除已经终止的 TCP 连接。在某些情况下，例如通信线路故障，TCP 连接或对方主机重启，TCP 连接实际已经终止，但是由于 TCP 连接上一直没有通信，系统无法及时发现这种情况，这时可以使用 clear tcp 命令关闭已经无效的 TCP 连接。其中，clear tcp local host-name port remote host-name port 命令用于终止指定的本地主机 IP 地址/端口和远端主机 IP 地址/端口之间的 TCP 连接。clear tcp tcb address 命令用于终止指定 TCB 地址所标识的 TCP 连接。

示例

下面的例子清除 192.168.20.22:23（本地）和 192.168.20.120:4420（远端）之间的 TCP 连接。show tcp brief 命令显示了当前 TCP 连接的本地和远端主机信息。

```
Router#show tcp brief
TCB          Local Address          Foreign Address        State
0xE85AC8      192.168.20.22:23       192.168.20.120:4420    ESTABLISHED
0xEA38C8      192.168.20.22:23       192.168.20.125:1583    ESTABLISHED
Router#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
Router#show tcp brief
TCB          Local Address          Foreign Address        State
0xEA38C8      192.168.20.22:23       192.168.20.125:1583    ESTABLISHED
```

下面的例子清除 TCB 地址为 0xea38c8 的 TCP 连接。show tcp brief 命令显示了 TCP 连接的 TCB 地址。

```
Router#show tcp brief
TCB          Local Address          Foreign Address        State
0xEA38C8      192.168.20.22:23       192.168.20.125:1583    ESTABLISHED
Router#clear tcp tcb 0xea38c8
Router#show tcp brief
TCB          Local Address          Foreign Address        State
```

相关命令

show tcp

show tcp brief

show tcp tcb

6.1.2 clear tcp statistics

清除 TCP 统计数据。

clear tcp statistics

参数

该命令没有参数或关键字。

命令模式

管理态

示例

用下列命令清除 TCP 统计数据：

Router#clear tcp statistics

相关命令

show tcp statistics

6.1.3 debug arp

显示 ARP 交互信息，例如发出 ARP 请求，收到 ARP 响应，收到 ARP 请求，发出 ARP 响应等。当路由器和主机无法通信时，可以用于分析 ARP 交互情况。用 no debug arp 停止显示信息。

debug arp

no debug arp

参数

该命令没有参数或关键字。

命令模式

管理态

示例

```
Router#debug arp
Router#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0
IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:
00:00:00:00:00, wrong cable, Ethernet1/1
IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0
IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0
IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0
```

第一条信息表明：路由器在接口 Ethernet 1/0 上收到一个 ARP 请求，发出请求的主机 IP 地址为 192.168.20.116，MAC 地址为 00:90:27:a7:a9:c2，它请求 IP 地址为 192.168.20.111 的主机的 MAC 地址：

IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

第二条信息表明：路由器在接口 Ethernet 1/1 上收到一个来自 192.168.20.139 的 ARP 地址请求。但是，根据路由器的接口配置，这个接口并不在这台主机所宣称的网络上。所以，可能是主机配置不正确。路由器如果根据这条信息建立了 ARP 缓存，就可能无法和连接在正常接口上的某台配置了相同地址的主机通信。

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:00:00:00:00:00, wrong cable, Ethernet1/1

第三条信息表明，路由器要解析主机 192.168.20.77 的 MAC 地址，所以在 ARP 缓存中为它建立了一条不完整的 ARP 表项，等收到 ARP 应答时再填入 MAC 地址。根据路由器的配置，这台主机连接在接口 Ethernet 1/0 上。

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

第四条信息表明，路由器在接口 Ethernet 1/0 上发出 ARP 请求，所带的路由器的 IP 地址是 192.168.20.22，接口的 MAC 地址是 08:00:3e:33:33:8a，所请求的主机 IP 地址是 192.168.20.77。这条信息和第三条信息是相关的。

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

第五条信息表明，路由器在接口 Ethernet1/0 上收到了 192.168.20.77 发给路由器接口 192.168.20.22 的 ARP 响应，告知它的 MAC 地址为 00:30:80:d5:37:e0。这条信息是和第三、四条信息相关的。

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

6.1.4 debug ip icmp

显示 Internet 控制信息协议（ICMP）的交互信息。使用命令 no debug ip icmp 关闭调试输出。

debug ip icmp

no debug ip icmp

参数

该命令没有参数或关键字。

命令模式

管理态

使用说明

该命令可以显示系统收到和发出的 ICMP 报文，从而解决网络端到端到的连接问题。如果要了解 debug ip icmp 命令输出的详细含义，请参见 RFC 792，“Internet Control Message Protocol”。

示例

```
Router#debug ip icmp
Router#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48
```

ICMP: rcvd echo from 192.168.20.125, len 40
ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40
ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36
ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

关于第一条信息的说明如下：

ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

域	描述
ICMP:	显示的是Internet控制信息协议（ICMP）报文的信息。
Sent	发送ICMP报文。
pointer indicating	ICMP报文类型，这个ICMP报文表示原始IP报文参数错误，并指出错误的域。其它类型的ICMP报文有： echo reply（回应应答） dst unreachable（目的不可到达），包括： ---net unreachable（网络不可到达） ---host unreachable（主机不可到达） ---protocol unreachable（协议不可到达） ---port unreachable（端口不可到达） ---fragmentation needed and DF set（需要分片，但DF位被置位） ---source route failed（源路由失败） ---net unknown（未知网络） ---destination host unknown（未知主机） ---source host isolated（源主机被隔离） ---net prohibited（与网络的通信被禁止） ---host prohibited（与主机的通信被禁止） ---net tos unreachable（对请求的服务类型，网络不可到达） ---host tos unreachable（对请求的服务类型，主机不可到达） source quench（源抑制） redirect（重定向），包括： ---net redirect（网络重定向） ---host redirect（主机重定向） ---net tos redirect（对服务类型和网络的重定向） ---host tos redirect（对服务类型和主机的重定向） echo（回应请求）

	router advertisement（路由器广告） router solicitation（路由器请求） time exceeded（超时），包括： ---ttl exceeded（ttl超时） ---reassembly timeout（重组超时） parameter problem（一般参数问题），包括： ---pointer indicating（指出错误参数） ---option missed（缺少选项） ---bad length（长度错误） timestamp（时戳） timestamp reply（时戳应答） information request（信息请求） information reply（信息应答） mask request（掩码请求） mask reply（掩码应答） 如果是系统未知的ICMP类型，系统将显示ICMP类型和代码的值。
to 192.168.20.124	ICMP报文的目的地址是192.168.20.124，这也是引起这个ICMP报文的原始报文的源地址。
(dst was 192.168.20.22)	引起ICMP报文的原始报文的目的地址是192.168.20.22。
len 48	ICMP报文的长度是48字节，其中不包括IP报头长度。

关于第二条信息的说明如下：

ICMP: rcvd echo from 192.168.20.125, len 40

域	描述
rcvd	收到ICMP报文。
echo	ICMP报文类型，是回应请求报文。
from 192.168.20.125	ICMP报文的源地址是192.168.20.125。

关于第三条信息的说明如下：

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

域	命令
src 192.168.20.22	ICMP报文的源地址是192.168.20.22。
dst 192.168.20.125	ICMP报文的目的地址是192.168.20.125。

根据 ICMP 报文类型的不同，产生的 ICMP 报文信息采用不同的格式，以便显示报文内容。

例如，对于 ICMP 重定向报文，采用下列格式打印：

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36
ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

其中第一条信息表示，收到来自主机 192.168.20.77 的 ICMP 主机重定向报文，建议使用网关 192.168.20.26 到达目的主机 22.0.0.3，ICMP 报文长度 36 字节。

第二条信息表示，发送 ICMP 主机重定向报文到 192.168.20.124，通知它使用网关 192.168.20.77 到达主机 22.0.0.5, ICMP 报文长度 36 字节。

对于 ICMP 目的不可到达报文，采用下列格式打印：

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36
ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

其中，第一条信息表示，路由器无法路由某个 IP 报文，所以向报文的源主机 192.168.20.124 发送 ICMP 目的主机（202.96.209.133）不可到达报文, ICMP 报文长度 36 字节。

第二条信息表示，路由器收到一个来自主机 192.168.20.26 的 ICMP 报文，通知目的主机（2.2.2.2）不可到达, ICMP 报文长度 36 字节。

6.1.5 debug ip packet

显示 Internet 协议（IP）的交互信息。使用 no debug ip packet 停止显示信息。

debug ip packet [**detail**] [*ip-access-list-name*]

no debug ip packet

参数

参数	参数说明
detail	（可选）输出IP报文封装的协议信息，如协议号，UDP、TCP端口号，ICMP报文类型等。
ip-access-list-name	（可选）用于过滤输出信息的IP访问表名称。只有满足指定IP访问表的IP报文的信息才会被输出。
access-group	（可选）用于过滤输出信息的IP访问表名称。只有满足指定IP访问表的IP报文的信息才会被输出。
interface	（可选）用于过滤输出信息的端口名称。只有满足指定端口的IP报文的信息才会被输出。

命令模式

管理态

使用说明

这条命令可以帮助了解每个收到的或是本地产生的 IP 报文的最终流向，了解通信发生问题的原因。

可能的情况有：

- 被转发

- 被作为广播报文或多播报文转发
- 转发时寻径失败
- 发送 redirect 报文
- 由于带有源路由选项被拒绝
- 由于非法的 IP options 被拒绝
- 源路由
- 本地发送报文需要分片，但是 DF 位被置位
- 收到报文
- 收到 IP 分片
- 发送报文
- 发送广播/多播
- 本地生成报文寻径失败
- 本地生成报文被分片
- 收到报文被过滤
- 发送报文被过滤
- 链路层封装失败（只限于以太网）
- 未知协议

使用这条命令可能会有大量的输出信息，所以最好在路由器比较空闲的时候使用，否则将严重影响系统性能。另外，尽可能使用访问表过滤输出，使系统只显示用户感兴趣的报文信息。

命令模式

管理态

示例

```
router#debug ip packet
router#IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected
IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending
IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, forward
IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd
```

域	描述
IP	表示这条信息是关于IP报文的。
s=192.168.20.120 (Ethernet1/0)	IP报文的源地址和收到报文的接口名称（如果不是本地生成的报文）。
d=19.0.0.9 (Ethernet1/0)	IP报文的目的地址和发送报文的接口名称（如果路由成功的话）。
g=192.168.20.1	IP报文的下一跳目的地址，可能是网关地址，也可能就是目的地址。

len	IP报文的长度。
redirected	表示路由器将向这个报文的源主机发送ICMP重定向报文。其它情况还有： forward---报文被转发。 forward directed broadcast---报文作为定向广播被转发，报文将在发送接口上转成物理广播。 unroutable---报文寻径失败，将被丢弃。 source route---源路由。 rejected source route---系统当前不支持源路由，因此拒绝带IP源路由选项的报文。 bad options---IP选项错误，报文被丢弃。 need frag but DF set---本地报文需要分片，但是DF被置位。 rcvd---报文被本地接收。 rcvd fragment---收到报文分片。 sending---发送本地生成报文。 sending broad/multicast---发送本地生成的广播/多播报文。 sending fragment---发送在本地分片的IP报文。 denied by in acl---被接收接口的接收访问表拒绝。 denied by out acl---被发送接口的发送访问表拒绝。 unknown protocol---未知协议。 encapsulation failed---协议封装失败，只限于以太网。当要在以太网接口上发送的报文由于ARP解析失败而被丢弃时，显示这条信息。

第一条信息表明，路由器收到一个 IP 报文，它的源地址是 192.168.20.120，来自接口 Ethernet1/0 所连接的网段，目的地址是 19.0.0.9，根据路由表确定的发送接口是 Ethernet1/0，网关地址是 192.168.20.1，报文长度为 60 字节。发现网关和发出 IP 报文的源主机直连在同一网络上，也就是路由器的接口 Ethernet1/0 所连接的网络上，所以路由器发出 ICMP 重定向报文。

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected

第二条信息，描述了 ICMP 重定向报文的发送，源地址是本地地址 192.168.20.22，目的地址是上述报文的源地址 192.168.20.120，从接口 Ethernet1/0 发出，由于是直接到达目的地，所以网关地址就是目的地址 192.168.20.120，ICMP 重定向报文长度为 56 字节。

IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending

第三条信息表明，IP 层收到一个 IP 报文，报文的源地址是 192.168.20.120，接收接口为 Ethernet1/0，报文的目的地址是 19.0.0.9，通过查找路由表，发现需要转发这个报文到接口 Ethernet1/0，网关是 192.168.20.77，报文长度为 60 字节。这条信息显示的是系统在发出 ICMP 重定向报文以后，转发第一条信息显示的报文。

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.77, len=60, forward

第四条信息表示，IP 层收到一个 IP 报文，源地址是 192.168.20.81，接收接口是 Ethernet1/0， 目的地址是 192.168.20.22，是在路由器接口 Ethernet1/0 上配置的一个 IP 地址，报文长度是 56 字节，本地接收。

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

下面介绍 debug ip packet detail 命令的输出，只说明其中新增的部分：

router#debug ip packet detail
router#IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67
IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89
IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0
IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

域	描述
UDP	协议名称，例如UDP, ICMP, TCP等。其它协议用协议号表示。
type, code	ICMP报文的类型和代码值。
src, dst	UDP和TCP报文的源端口和目的端口。
seq	TCP报文的序列号。
ack	TCP报文的确认号。
win	TCP报文的窗口值。
ACK	TCP报文的控制比特中ACK被置位，表明确认序列号有效。其它的控制比特是SYN, URG, FIN, PSH, RST。

第一条信息表明，收到 UDP 报文，源端口是 68，目的端口是 67。

IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

第二条信息表明，收到报文的协议号为 89。

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

第三条信息表明，收到 ICMP 报文，报文类型为 0，代码为 0。

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

第四条信息表明，发送 TCP 报文，源端口为 1024，目的端口为 23，序列号为 75098622，确认号为 161000466，接收窗口尺寸为 17520，ACK 标志位被置位。关于这些域的含义，请参见 RFC 793— TRANSMISSION CONTROL PROTOCOL。

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

下面介绍如何使用访问控制表。例如，要求只显示源地址是 192.168.20.125 的报文信息，首先定义标准访问控制表 abc，只允许源地址是 192.168.20.125 的 IP 报文。然后，在 debug ip packet 命令中使用该访问控制表。

Router#config
Router_config#ip access-list standard abc
Router_config_std_nacl#permit 192.168.20.125
Router_config_std_nacl#exit
Router_config#exit

```
Router#debug ip packet abc
Router#IP: s=192.168.20.125 (Ethernet0/1), d=192.168.20.22 (Ethernet0/1), len=48, rcvd
```

上述命令使用的是标准的访问控制表，也可以使用扩展访问控制表。

相关命令

debug ip tcp packet

6.1.6 debug ip raw

显示 Internet 协议（IP）的交互信息。使用 no debug ip raw 停止显示信息。

debug ip raw [**detail**] [**access-list-group**] [**interface**]

no debug ip raw

参数

参数	参数说明
detail	（可选）输出IP报文封装的协议信息，如协议号，UDP、TCP端口号，ICMP报文类型等。
access-group	（可选）用于过滤输出信息的IP访问表名称。只有满足指定IP访问表的IP报文的信息才会被输出。
interface	（可选）用于过滤输出信息的端口名称。只有满足指定端口的IP报文的信息才会被输出。

命令模式

管理态

使用说明

这条命令可以帮助了解每个收到的或是本地产生的 IP 报文的最终流向，了解通信发生问题的原因。

可能的情况有：

- 被转发
- 被作为广播报文或多播报文转发
- 转发时寻径失败
- 发送 redirect 报文
- 由于带有源路由选项被拒绝
- 由于非法的 IP options 被拒绝
- 源路由
- 本地发送报文需要分片，但是 DF 位被置位
- 收到报文
- 收到 IP 分片

- 发送报文
- 发送广播/多播
- 本地生成报文寻径失败
- 本地生成报文被分片
- 收到报文被过滤
- 发送报文被过滤
- 链路层封装失败（只限于以太网）
- 未知协议

使用这条命令可能会有大量的输出信息，所以最好在路由器比较空闲的时候使用，否则将严重影响系统性能。另外，尽可能使用访问表过滤输出，使系统只显示用户感兴趣的报文信息。

示例

与 debug ip packet 一至，故略。

相关命令

debug ip tcp packet

6.1.7 debug ip rtp

显示头部压缩的交互信息。使用 no debug ip rtp 停止显示信息。

debug ip rtp {**header-compression|packets |rtcp**}

no debug ip rtp {**header-compression|packets |rtcp**}

参数

参数	参数说明
header-compress	RTP/UDP/IP头部压缩事件。
packets	RTP/UDP/IP头部压缩交互数据报。
rtcp	TCP/IP头部压缩交互数据报。

命令模式

管理态

使用说明

这条命令可以帮助了解头部压缩交互的具体过程。

使用这条命令可能会有大量的输出信息，所以最好在路由器比较空闲的时候使用，否则将严重影响系统性能。

示例

```
router # debug ip rtp header-compress
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: new connection, conn 0,
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7078, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7079, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7080, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7081, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7082, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7083, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7084, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7085, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7086, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4024, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7087, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4025, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4026, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7088, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7089, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4027, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7090, Gen =
0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4028, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7091, Gen =
0
2002-1-9 21:36:42
```

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4029, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7092, Gen = 0
2002-1-9 21:36:42
21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4030, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7093, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7094, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4032, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7095, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4033, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7096, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4034, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7097, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7098, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4036, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7099, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4037, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7100, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4038, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7101, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: tossing error packet
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7102, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4040, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7103, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4041, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7104, Gen = 0

```
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4042, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7105, Gen =
0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7106, Gen =
0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4044, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7107, Gen =
0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4045, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7108, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4046, Gen = 0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7109, Gen =
0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7110, Gen =
0
2002-1-9 21:36:43
21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4048, Gen = 0
no deb all
```

6.1.8 debug ip tcp packet

显示传输控制协议（TCP）报文的收发信息。用 no debug ip tcp packet 停止显示。

debug ip tcp packet

no debug ip tcp packet

参数

该命令没有参数或关键字。

命令模式

管理态

示例

```
Router#debug ip tcp packet
Router#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
        DATA 1 ACK 3130379810 PSH WIN 4380
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
        DATA 2 ACK 50659460 PSH WIN 16372
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
        DATA 50 ACK 3130379812 PSH WIN 4380
tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
        ACK 3130379812 FIN WIN 4380
```

```
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659511 WIN 16321
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
        ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
        DATA 2 ACK 8057944 PSH WIN 17440
tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944
        RST
```

域	描述
tcp:	表示关于TCP报文的信息。
O	发送TCP报文。
ESTABLISHED	TCP连接的当前状态。关于TCP连接状态的描述，参见debug ip tcp transactions命令说明。
192.168.20.22:23	报文的源地址是192.168.20.22，源端口是23。
192.168.20.125:3828	报文的目的地址是192.168.20.125，目的端口是3828。
seq 50659460	报文的序列号是50659460。
DATA 1	报文包含的有效数据字节数是1个。
ACK 3130379810	报文的确认号是3130379810。
PSH	报文的控制比特中PSH被置位。 其它的控制比特位有ACK, FIN, SYN, URG, RST。
WIN 4380	报文的窗口域用于通知对方接收端接收缓存区大小，目前是4380字节。
I	接收TCP报文。

如果上述某些域没有出现在显示中，说明在这个 TCP 报文中该域没有有效值。

相关命令

debug ip tcp transactions

6.1.9 debug ip tcp transactions

显示传输控制协议（TCP）的重要交互信息，例如 TCP 连接状态改变等。用 no debug ip tcp transactions 停止显示。

debug ip tcp transactions

no debug ip tcp transactions

参数

该命令没有参数或关键字。

命令模式

管理态

示例

```
Router#debug ip tcp transactions
Router#TCP: rcvd connection attempt to port 23
TCP: TCB 0xE88AC8 created
TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]
TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]
TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]
TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]
TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]
TCP: TCB 0xE923C8 deleted
TCP: TCB 0xE7DBC8 created
TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT
TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]
TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]
TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]
TCP: sending FIN [1022 -> 192.168.20.124:513]
TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]
TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]
TCP: TCB 0xE7DBC8 deleted
```

域	描述
TCP:	表示显示TCP交互信息。
rcvd connection attempt to port 23	收到对端口23（telnet端口）的连接请求。
TCB 0xE88AC8 created	生成一个新的TCP连接控制块，其标识为0xE88AC8。
state was LISTEN -> SYN_RCVD	表示TCP状态机的状态从LISTEN转到SYN_RCVD。 可能的TCP状态有: LISTEN---等待来自任意远端主机的TCP连接请求。 SYN_SENT---发出连接请求以发起TCP连接协商，正在等待对方的应答。 SYN_RCVD---收到对方的连接请求并发出确认，也发出了自己的连接请求，正在等待对方的连接请求确认。 ESTABLISHED---表示连接建立成功，处于数据传送阶段，可以收发上层应用的数据。 FIN_WAIT_1---已经向对方发出连接终止请求，等待对方的确认，以及对方的连接终止请求。 FIN_WAIT_2---已经向对方发出连接终止请求，并收到对方的确认，正在等待对方的连接终止请求。 CLOSE_WAIT---收到对方的连接终止请求，发出确认，正在等待本地用户关

	闭连接，一旦用户要求关闭连接，系统将发出连接终止请求。 CLOSING---已经向对方发出连接终止请求，也收到对方的连接终止请求并发出确认，正在等待对方对本地连接终止请求的确认。 LAST_ACK---已经收到对方的连接终止请求并确认，发出连接终止请求，正在等待确认。 TIME_WAIT---正在等待足够的时间以确定对方收到了本地对它的连接终止请求的确认，以及仍在网络中传输的有关这个连接的报文到达目的地或是被丢弃。 CLOSED---表示完全没有连接或者连接已经完全关闭。 如果要了解更为详细的信息，请参阅RFC 793，TRANSMISSION CONTROL PROTOCOL。
[23 -> 192.168.20.125:3828]	在括号中： 第一个域（23）表示本地TCP端口。 第二个域（192.168.20.125）表示远端IP地址。 第三个域（3828）表示远端TCP端口。
sending SYN	发出一个连接请求报文（TCP报头控制比特中的SYN置位）。其它的TCP控制比特包括SYN, ACK, FIN, PSH, RST和URG。
seq 50658312	发出报文的序列号为50658312。
ack 3130379657	发出报文的确认号为3130379657。
rcvd FIN	收到连接终止请求（TCP报头控制比特中的FIN置位）。
connection closed by user	上层应用要求关闭TCP连接。
connection timed out	连接超时被关闭。

相关命令

debug ip tcp packet

6.1.10 debug ip udp

显示用户数据报协议（UDP）的交互信息。使用命令 no debug ip udp 停止显示。

debug ip udp

no debug ip udp

参数

该命令没有参数或关键字。

命令模式

管理态

示例

```
Router#debug ip udp
Router#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32
UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008
```

域	描述
UDP:	表示这条信息是关于UDP报文的。
rcvd	收到报文。
sent	发出报文。
src	UDP报文的源IP地址和UDP端口。
dst	UDP报文的目的IP地址和UDP端口。
len	UDP报文的长度。

所以，第一条信息说明收到一个 UDP 报文，来自主机 192.168.20.99，端口为 520，目的地址是 192.168.20.255，目的端口是 520，报文长度为 32 字节。

第二条信息说明发出一个 UDP 报文，本地地址是 192.168.20.22，端口是 20001，目的地址是 192.168.20.43，目的端口是 1001，报文长度为 1008 字节。

6.1.11 ip mask-reply

要求路由器在指定接口上回应 IP 地址掩码请求。如果要关闭这项功能，使用 no ip mask-reply。

ip mask-reply

no ip mask-reply

default ip mask-reply

参数

该命令没有参数或关键字。

缺省

不应答 IP 地址掩码请求。

命令模式

接口配置态

示例

```
interface ethernet 1/1
ip mask-reply
```

6.1.12 ip mtu

设置接口发出的 IP 报文的最大发送单元（MTU）长度，使用 ip mtu 命令。如果要重新使用 MTU 缺省值，使用 no ip mtu 命令。

ip mtu bytes

no ip mtu

参数

参数	参数说明
bytes	以字节计算的IP最大传输长度。

缺省

根据接口物理介质的不同，和接口上的最大传输长度（mtu）相同。最小是 68 字节。

命令模式

接口配置态

使用说明

如果 IP 报文长度超过接口设置的 IP MTU，路由器将对报文分片。所有连在同一物理介质上的设备，应该设置相同的协议 MTU 才能通信。MTU 值（通过接口配置命令 mtu 设置）会影响 IP MTU 值。如果 IP MTU 值和 MTU 值相同，当改变 MTU 值时，IP MTU 的值会自动改变为新的 MTU 值。反之，改变 IP MTU 值不会影响 MTU 值。

IP MTU 最小值为 68 字节，最大值不超过接口配置的 MTU。

示例

下列命令把接口的 IP MTU 设为 200：

```
interface serial0/0
ip mtu 200
```

相关命令

mtu

6.1.13 ip redirects

发送 IP ICMP 重定向报文。不发送 ICMP 重定向报文，用命令 no ip redirects。

ip redirects

no ip redirects

参数

命令没有参数或关键字。

缺省

一般情况下，IP 重定向报文是缺省被发送的。但是，如果用户在接口上配置了热备份路由器协议，该项功能将被自动关闭。而且，如果以后热备份路由器协议的配置被取消，这项功能不会自动打开。

命令模式

接口配置态

使用说明

当路由器在转发报文时发现网关所在的转发接口和收到报文的接口相同，而且发送报文的主机就直连在这个接口的逻辑网络上的话，根据协议，它可以发出一个 ICMP 重定向报文，通知源主机直接把那个路由器作为到报文目的地址的网关，而不再经过这台路由器转发。

如果接口配置了热备份路由器协议，发送 IP 重定向报文可能导致报文丢失。

示例

下面的命令在接口 ethernet1/0 上打开发送 ICMP 重定向报文的功能：

```
interface ethernet 1/0
ip redirects
```

6.1.14 ip route cache

查询路由的时候，允许对查找到的路由按照流创建路由缓存。如果不允许创建路由缓存，使用no ip route cache 配置命令。

ip route cache [age_time *value* | [fast | acl] | hash_bit *value* | link_cnt *value***]**

no ip route cache

参数

参数	参数说明
age_time	cache 老化时间，取值 2~8 秒，默认 5 秒
fast	不支持负载均衡的快速 cache
acl	支持基于 ip 五元组的 cache
hash_bit	hash 数组的大小为 1 << hash_bit，取值 1~16，默认为 12
link_cnt	hash 冲突链的长度，取值 1~16，默认为 4

缺省

允许查找的路由按照流进行cache。

命令模式

全局配置态

使用说明

如果要禁止查找到的路由被cache，需要显示配置no ip route cache。

可以创建的路由cache 条目数为： link_cnt * 2^hash_size。

示例

这个例子配置禁止进行路由cache：

```
R1_config#no ip route cache
```

相关命令

无

6.1.15 ip source-route

允许路由器处理带 IP 源路由选项的 IP 报文。如果要求路由器丢弃任何带 IP 源路由选项的 IP 报文，使用 no ip source-route 命令。

ip source-route

no ip source-route

参数

该命令没有参数或关键字。

缺省

处理带 IP 源路由选项的 IP 报文。

命令模式

全局配置态

示例

下列命令要求处理带 IP 源路由选项的 IP 报文：

ip source-route

相关命令

ping

6.1.16 ip tcp synwait-time

设置路由器等待 TCP 连接成功的超时时间。如果要回到缺省时间，使用 no ip tcp synwait-time 命令。

ip tcp synwait-time *seconds*

no ip tcp synwait-time

参数

参数	参数说明
seconds	以秒为单位的TCP连接等待时间。有效取值在5 ~ 300秒之间。缺省是75秒。

缺省

75 秒

命令模式

全局配置态

使用说明

当路由器发起 TCP 连接时，如果在 TCP 连接等待时间之后连接仍没有建立成功，则路由器认为连接失败，并把这一结果返回给上层应用程序。用户可以设置 TCP 等待连接建立成功的时间，缺省是 75 秒。这个选项与经过路由器转发的 TCP 连接报文无关，而只与路由器本机的 TCP 连接有关。

如果要知道当前值，使用命令 ip tcp synwait-time ?，在方括号[]中的值就是当前值。

示例

下面的例子把 TCP 连接等待时间设为 30 秒：

```
Router_config#ip tcp synwait-time 30
Router_config#ip tcp synwait-time ?
  <5-300>[30] seconds        -- wait time
```

6.1.17 ip tcp window-size

设置 TCP 窗口尺寸。 如果要回到缺省值，使用 no ip tcp window-size 命令。

ip tcp window-size bytes

no ip tcp window-size

参数

参数	参数说明
bytes	以字节为单位的窗口尺寸。最大是65535字节。缺省是2000字节。

缺省

2000 字节

命令模式

全局配置态

使用说明

除非明确知道为什么要改变缺省值，否则不要轻易改变。如果要知道当前值，使用命令 ip tcp window-size ?，在方括号[]中的值就是当前值。

示例

下面的例子把 TCP 窗口尺寸设为 6000 字节：

```
Router_config#ip tcp window-size 6000
Router_config#ip tcp window-size ?
  <1-65535>[6000] bytes        -- Window size
```

6.1.18 ip unreachables

设置路由器发出 ICMP 不可到达报文。如果要求路由器停止发送，使用 no ip unreachables 命令。

ip unreachable

no ip unreachable

参数

该命令没有参数或者关键字。

缺省

发送 ICMP unreachable 报文。

命令模式

接口配置态

使用说明

路由器在转发 IP 报文的时候，可能发现路由表中没有相关路由，导致报文被丢弃，这时，路由器可以向源主机发出 ICMP 不可到达报文，通知源主机这一情况，以便源主机及时发现错误，并进行更正。

示例

下面的例子设置在接口 ethernet 1/0 上发送 ICMP 不可到达报文：

```
interface ethernet 1/0
ip unreachables
```

6.1.19 ip vrf forwarding

设置路由器接口所属的 VRF。

ip vrf forwarding *vrfname*

no ip vrf forwarding *[vrfname]*

参数

参数	参数说明
vrfname	VRF名字

缺省

不属于任何 VRF。

命令模式

接口配置态

使用说明

必须先有 VRF 才能配置该命令，且该命令会删除接口下的 ip 地址配置，所以在接口上要先用该命令指定 VRF，然后再配置 ip 地址。

示例

下面的例子设置接口 g0/0 属于 VRF“vpn1”：

```
interface g0/0
ip vrf forwarding vpn1
```

6.1.20 ip error-log

记录因为各种错误原因丢弃的报文。

ip error-log

no ip error-log

参数

该命令没有参数或者关键字。

缺省

不输出任何信息。

命令模式

全局配置态

使用说明

当因为某些错误原因丢弃报文时，通过打开该命令可以看到相关日志信息。

示例

下面的例子启用该功能：

ip error-log

6.1.21 ip check-noncidr

启用非 CIDR 模式下的目的地址检查。

ip check-noncidr

no ip check-noncidr

参数

该命令没有参数或者关键字。

缺省

不启用该功能。

命令模式

全局配置态

使用说明

从非 CIDR 角度检查目的地址，如 host 字段为 0 的话，将会丢弃该报文

示例

下面的例子启用该功能：

ip check-noncidr

6.1.22 show ip cache

显示用于 IP 快速交换的路由缓存。

show ip cache [*prefix mask*] [*type number*]

参数

参数	参数说明
prefix mask	（可选）只显示表项的目的地址和用户所键入指定的前缀/掩码相匹配的表项。
type number	（可选）只显示表项的发送接口和用户所键入指定的接口类型/编号相匹配的表项。

rsvp	（可选）只显示与RSVP相关的表项，说明此表项RSVP正在使用。

命令模式

管理态

示例

下面的例子显示路由缓存：

```
Router#show ip cache
Source          Destination     Interface       Next Hop
192.168.20.125  2.0.0.124       Serial1/0       2.0.0.124
192.168.20.124  192.168.30.124  Serial1/0       2.0.0.124
2.0.0.124       192.168.20.125  Ethernet1/1     192.168.20.125
```

域	描述
Source	源地址。
Destination	目的地址。
Interface	发送接口的类型和编号。
Next Hop	网关地址。

下面的例子显示目的地址和指定前缀/掩码匹配的路由缓存：

```
Router#show ip cache 192.168.20.0 255.255.255.0
Source          Destination     Interface       Next Hop
2.0.0.124       192.168.20.125  Ethernet0/1     192.168.20.125
```

下面的例子显示发送接口和指定的接口类型/掩码匹配的路由缓存：

```
Router#show ip cache s1/0
Source          Destination     Interface       Next Hop
192.168.20.125  2.0.0.124       Serial1/0       2.0.0.124
192.168.20.124  192.168.30.124  Serial1/0       2.0.0.124
```

6.1.23 show ip irdp

显示 irdp protocl 信息。

参数

该命令没有参数或者关键字。

命令模式

管理态

示例

```
xuhao_config_e1/0#   show ip irdp
Async0/0 ICMP router discovery protocol(IRDP) : OFF

Ethernet1/0 ICMP router discovery protocol(IRDP) : ON
```

Advertisements occur between every 450 and 600 seconds
Advertisements are sent as broadcasts
Advertisements valid in 1800 seconds
Default preference : 0

Ethernet1/1 ICMP router discovery protocol(IRDP) : OFF

Null0 ICMP router discovery protocol(IRDP) : OFF

Loopback7 ICMP router discovery protocol(IRDP) : OFF

Loopback10 ICMP router discovery protocol(IRDP) : OFF

6.1.24 show ip sockets

显示 socket 信息。

show ip sockets

参数

该命令没有参数或者关键字。

命令模式

管理态

示例

Router#show ip sockets

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

域	描述
Proto（协议）	IP协议号。17是UDP，6是TCP。
Remote（远端）	远端地址。
Port（端口）	远端端口。
Local（本地）	本地地址。
Port（端口）	本地端口。
In（接收）	接收字节总数。
Out（发送）	发送字节总数。

6.1.25 show ip traffic

显示 IP 流量统计信息。

show ip traffic

参数

该命令没有参数或者关键字。

命令模式

管理态

示例

```
Router#show ip traffic
IP statistics:
Rcvd:  0 total, 0 local destination, 0 delivered
         0 format errors, 0 checksum errors, 0 bad ttl count
         0 bad destination address, 0 unknown protocol, 0 discarded
         0 filtered , 0 bad options, 0 with options
  Opts:  0 loose source route, 0 record route, 0 strict source route
         0 timestamp, 0 router alert, 0 others
  Frags: 0 fragments, 0 reassembled, 0 dropped
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 0 received, 0 sent
  Mcast: 0 received, 0 sent
  Sent:  230 generated, 0 forwarded
         0 filtered, 0 no route, 0 discarded
ICMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 redirect, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements
Sent: 0 total, 0 errors
0 redirects, 0 unreachable, 0 source quench
0 echos, 0 echo replies, 0 mask requests, 0 mask replies
0 parameter problem, 0 timestamps, 0 timestamp replies
0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:
Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock
Sent: 0 total

TCP statistics:
Rcvd: 0 total, 0 checksum errors, 0 no port
Sent: 3 total

IGMP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors
0 host queries, 0 host reports
Sent: 0 host reports
```

ARP statistics:
Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other
Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse

域	描述
format errors（格式错误）	报文格式错误，例如IP报头长度错误
bad hop count（TTL错误）	路由器在转发报文时，发现报文的TTL值被减到0。报文将被丢弃。
no route（没有路由）	路由器没有相应路由的报文。

6.1.26 show tcp

显示所有 TCP 连接的状态信息。

show tcp

参数

该命令没有参数或者关键字。

命令模式

管理态

示例

```
Router#show tcp

TCB 0xE9ADC8
Connection state is ESTABLISHED, unread input bytes: 934
Local host: 192.168.20.22, Local port: 1023
Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934    mis-ordered: 0 (0 packets)

Timer          Starts    Wakeups          Next(ms)
Retrans            33          1                 0
TimeWait            0          0                 0
SendWnd             0          0                 0
KeepAlive         102          0           7199500

iss:  29139463  snduna:  29139525  sndnxt:  29139525    sndwnd:    17520
irs: 709124039  rcvnxt: 709205436  rcvwnd:     4380

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61
```

域	描述
TCB 0xE77FC8	TCP连接控制块的内部标识。
Connection state is ESTABLISHED	TCP连接当前状态。TCP连接可能处于下列任一状态： LISTEN---等待来自任意远端主机TCP连接请求。 SYN_SENT---发出连接请求后，等待对方的应答。 SYN_RCVD---收到对方的连接请求并发出确认，也发出了自己的连接请求，正在等待对方的连接请求确认。 ESTABLISHED---表示连接建立成功，处于数据传送阶段，可以收发上层应用的数据。 FIN_WAIT_1---已经向对方发出连接终止请求，等待对方的确认，以及对方的连接终止请求。 FIN_WAIT_2---已经向对方发出连接终止请求，并收到对方的确认，正在等待对方的连接终止请求。 CLOSE_WAIT---收到对方的连接终止请求，发出确认，正在等待本地用户关闭连接，一旦用户要求关闭连接，系统将发出连接终止请求。 CLOSING---已经向对方发出连接终止请求，也收到对方的连接终止请求并发出确认，正在等待对方对本地连接终止请求的确认。 LAST_ACK---已经收到对方的连接终止请求并确认，发出连接终止请求，正在等待确认。 TIME_WAIT---正在等待足够的时间以确定对方收到了本地对它的连接终止请求的确认 CLOSED---表示完全没有连接或者连接已经完全关闭 如果要了解更为详细的信息，请参阅RFC 793，TRANSMISSION CONTROL PROTOCOL。
unread input bytes:	经下层TCP处理后可以提交给上层应用，但是上层应用还没有接收的数据。
Local host:	本地IP地址。
Local port:	本地TCP端口。
Foreign host:	远端IP地址。
Foreign port:	远端TCP端口。
Enqueued bytes for transmit:	发送队列中的字节数，包括已经发送但还没有被对方确认的数据和还没有发送的数据。
input:	接收队列中的字节数，这些数据经过排序后等待被上层应用接收。
mis-ordered:	错序队列中的字节数和报文数，这些数据必须等待其它的一些数据收到后，才能顺序进入接收队列被上层应用接收。例如，收到报文1，2，4，5和6，报文1和2可以进入接收队列，但是4，5和6只能进入错序队列等待报文3的到达。

接着显示当前连接的定时器使用情况，包括定时器启动的次数，定时器超时的次数和定时器距离下次超时的时间（0 表示定时器当前不再运行）。每个连接都使用独立的定时器。定时器的超时次数一般小于定时器的启动次数，因为定时器在运行过程中有可能被重置。例如，重发定时器运行时系统收到对方对所有发送数据的确认，重发定时器将停止运行。

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

域	描述
Timer	定时器名称。
Starts	定时器的启动次数。
Wakeups	定时器的超时次数。
Next(ms)	定时器距离下次超时的时间（以毫秒为单位），0表示定时器不在运行。
Retrans	重发定时器，用于触发数据重发。定时器在发送数据后被启动，如果超时时间内数据未被对方确认，则重发数据。
TimeWait	时间等待定时器，用于确保对方收到连接终止请求确认。
SendWnd	发送窗口定时器，用于确保发送窗口在TCP确认丢失的情况下恢复到正常大小。
KeepAlive	保持活动定时器，用于确保通信链路正常和对方仍旧处于连接状态。它将触发测试报文的发送，以检测通信链路状态和对方状态。

接着显示 TCP 连接使用的序列号。TCP 使用序列号来保证可靠有序的数据传输。本地和远端主机还根据序列号来进行流量控制和发送确认。

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520
irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

域	描述
iss:	初始发送序列号。
snduna:	已经发送但是还没有收到对方确认的数据的第一个字节的发送序列号。
sndnxt:	以后发送的数据的第一个字节的发送序列号。
sndwnd:	远端主机的TCP窗口尺寸。
irs:	初始接收序列号，也就是远端主机的初始发送序列号。
rcvnxt:	最近确认的接收序列号。
rcvwnd:	本地主机的TCP窗口尺寸。

接着显示本地主机记录的发送时间，系统可以根据这些数据调整系统以适应不同的网络。

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

域	描述
SRTT:	平滑处理后的往返时间。

RXT:	重传超时时间。
RTV:	往返时间的变化值。
MinRXT:	允许的最小重传超时。
MaxRXT:	允许的最大重传超时。
ACK hold:	延迟确认以便和数据一起发送的最大延迟时间。

Datagrams (max data segment is 1460 bytes):
Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396
Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

域	描述
max data segment is	该连接允许的最大数据段长度。
Rcvd:	本地主机在这个连接过程中收到的报文数，以及其中错序的报文数。
with data:	包含有效数据的报文数。
total data bytes:	报文中包含的数据字节数。
Sent:	本地主机在这个连接过程中发送的报文总数，以及重发的报文数。
with data:	包含有效数据的报文数。
total data bytes:	报文中包含的数据字节数。

相关命令

show tcp brief

show tcp tcb

6.1.27 show tcp brief

显示 TCP 连接的简要信息。

show tcp brief [**all**]

参数

参数	参数说明
all	（可选）显示所有端口。如果不输入这个关键字，系统不显示处于LISTEN状态的端口。

命令模式

管理态

示例

```
Router#show tcp brief
TCB        Local Address        Foreign Address        State
```

0xE9ADC8 192.168.20.22:1023 192.168.20.124:513 ESTABLISHED
0xEA34C8 192.168.20.22:23 192.168.20.125:1472 ESTABLISHED

域	描述
TCB	TCP连接的内部标识。
Local Address	本地IP地址和TCP端口。
Foreign Address	远端IP地址和TCP端口。
State	连接状态。详细说明参见show tcp命令。

相关命令

show tcp

show tcp tcb

6.1.28 show tcp statistics

显示 TCP 统计数据。

show tcp statistics

参数

该命令没有参数或者关键字。

命令模式

管理态

示例

```
Router#show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 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 with unsend data
127 ack packets (247 bytes)
Sent: 239 Total, 0 urgent packets
6 control packets
123 data packets (245 bytes)
0 data packets (0 bytes) retransmitted
110 ack only packets (101 delayed)
0 window probe packets, 0 window update packets
4 Connections initiated, 0 connections accepted, 2 connections established
3 Connections closed (including 0 dropped, 1 embryonic dropped)
5 Total rxmt timeout, 0 connections dropped in rxmt timeout
```

1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive

域	描述
Rcvd:	关于路由器收到报文的统计数据。
Total	收到报文总数。
no port	收到报文中目的端口不存在的报文数。
checksum error	收到报文中校验和错误的报文数。
bad offset	收到报文中数据偏移量错误的报文数。
too short	收到报文中长度小于最小有效长度的报文数。
packets in sequence	按序收到的数据报文数。
dup packets	收到的重复报文数。
partially dup packets	收到的部分重复的报文数。
out-of-order packets	不是按顺序收到的报文数。
packets with data after window	收到的报文中数据超出路由器的接收窗口的报文数。
packets after close	连接关闭后收到的报文数。
window probe packets	收到的窗口探测报文数。
window update packets	收到的窗口更新报文数。
dup ack packets	收到的重复确认报文数。
ack packets with unsent data	收到的确认未发送数据的报文数。
ack packets	收到的确认报文数。
Sent	关于路由器发出报文的统计数据。
Total	发出报文总数。
urgent packets	发出的紧急报文数。
control packets	发出的控制（SYN、FIN或RST）报文数。
data packets	发出的数据报文数。
data packets retransmitted	重发的数据报文数。
ack only packets	发出的纯确认报文数。
window probe packets	发出的窗口探测报文数。
window update packets	发出的窗口更新报文数。
Connections initiated	本地发起的连接数。
connections accepted	本地接受的连接数。
connections established	本地建立连接数。

Connections closed	本地关闭连接数。
Total rxmt timeout	重发超时总数。
Connections dropped in rxmit timeout	重发超时导致的连接断开数。
Keepalive timeout	Keepalive超时数。
keepalive probe	发出的Keepalive探测报文数。
Connections dropped in keepalive	由于Keepalive被断开的连接数。

相关命令

clear tcp statistics

6.1.29 show tcp tcb

显示某个 TCP 连接的状态信息。

show tcp tcb address

参数

参数	参数说明
address	要显示的TCP连接的传输控制块(TCB)地址。TCB是系统内部对TCP连接的标识，可以用命令show tcp brief得到。

命令模式

管理态

示例

下列显示的具体说明参见 show tcp 命令。

```
Router_config#show tcp tcb 0xea38c8

TCB 0xEA38C8
Connection state is ESTABLISHED, unread input bytes: 0
Local host: 192.168.20.22, Local port: 23
Foreign host: 192.168.20.125, Foreign port: 1583

Enqueued bytes for transmit: 0, input: 0    mis-ordered: 0 (0 packets)

Timer          Starts     Wakeups          Next(ms)
Retrans          4          0                0
TimeWait         0          0                0
SendWnd          0          0                0
KeepAlive       +5          0             6633000

iss:  10431492   snduna:  10431573   sndnxt:  10431573     sndwnd:     17440
irs: 915717885   rcvnxt: 915717889   rcvwnd:     4380
```

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms
minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):
Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3
Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80

相关命令

show tcp

show tcp brief

6.2 访问列表配置命令

访问列表配置命令包括：

- deny
- ip access-group
- ip access-list
- permit
- show ip access-list

6.2.1 deny

在 IP 访问列表配置模式中可使用此命令配置禁止规则，要从 IP 访问列表中删除 deny 规则，在命令前加 no 前缀。

deny source [*source-mask*] [**log**]

no deny source [*source-mask*] [**log**]

deny protocol source *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos tos**] [**log**]

no deny protocol source *source-mask* **destination** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于互联网控制报文协议(ICMP)，也可以使用以下句法:

deny icmp source *source-mask* **destination** *destination-mask* [**icmp-type**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于 Internet 组管理协议(IGMP)，可以使用以下句法:

deny igmp source *source-mask* **destination** *destination-mask* [**igmp-type**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于 TCP，可以使用以下句法:

deny tcp source *source-mask* [**operator port**] **destination** *destination-mask* [**operator port**] [**established**] [**precedence** *precedence*] [**tos** *tos]* [**log**]

对于数据报协议(UDP)，可以使用以下句法:

deny udp source *source-mask* [**operator port**] **destination** *destination-mask* [**operator** *port*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

参数

参数	参数说明
protocol	协议名字或IP协议号。它可以是关键字icmp、igmp、igrp、ip、ospf、tcp或udp，也可以是表IP协议号的0到255的一个整数。为了匹配任何Internet协议(包括ICMP、TCP和UDP)使用关键字ip。某些协议允许进一步限定，如下描述。
source	源网络或主机号。有两种方法指定源：32位二进制数，用四个点隔开的十进制数表示。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
source-mask	源地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
destination	目标网络或主机号。有两种方法指定： 使用四个点隔开的十进制数表示的32位二进制数。 使用关键字any作为0.0.0.0 0.0.0.0的目标和目标掩码的缩写。
destination-mask	目标地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的目标地址和目标地址掩码缩写。
precedence precedence	(可选)包可以由优先级过滤，用0到7的数字指定。
tos tos	(可选) 数据包可以使用服务层过滤。使用数字0－15指定。
icmp-type	(可选)ICMP包可由ICMP报文类型过滤。类型是数字0到255。
igmp-type	(可选)IGMP包可由IGMP报文类型或报文名过滤。 类型是0到15的数字。
operator	(可选)比较源或目标端口。操作包括lt(小于)， gt(大于)，eq(等于)，neq(不等于)。如果操作符放在source和source-mask之后，那么它必须匹配这个源端口。如果操作符放在destination和destination-mask之后，那么它必须匹配目标端口。
port	(可选)TCP或UDP端口的十进制数字或名称。端口号是一个0到65535的数字。TCP端口名列在“使用方针”部分。当过滤TCP时，可以只使用TCP端口名称。UDP端口名称也列在“使用说明”部分。当过滤TCP时，只可使用TCP端口名。当过滤UDP时， 只可使用UDP端口名。
established	(可选)只对TCP协议，表示一个已建立的连接。如果TCP数据报ACK或RST位设置时，出现匹配。非匹配的情况是初始化TCP数据报，以形成一个连接。
log	(可选)可以进行日志记录。

命令模式

IP 访问列表配置态

使用说明

可以使用访问表控制包在接口上的传输，控制虚拟终端线路访问以及限制路由选择更新的内容。在匹配发生以后停止检查扩展的访问表。分段 IP 包，而不是初始段，立即由任何扩展的 IP 访问表接收。扩展的访问表用于控制访问虚拟终端线路或限制路由选择更新的内容，不必匹配 TCP 源端口、服务值的类型或包的优先权。

注意：

在初始建立一个访问表后，任何后续的添加内容(可能由终端键入)放置在列表的尾部。

以下显示用于替换端口号的 TCP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个？替代端口号的方式来寻找。

- bgp
- ftp
- ftp-data
- login
- pop2
- pop3
- smtp
- telnet
- www

以下显示用于替换端口号的 UDP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个？替代端口号的方式来寻找。

- domain
- snmp
- syslog
- tftp

示例

下面示例禁止 192.168.5.0 这个网段：

```
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
```

注意：

IP 访问表由一个隐含的 deny 规则结束。

相关命令

ip access-group

ip access-list

permit

show ip access-list

6.2.2 ip access-group

为了控制访问一个接口,使用 ip access-group 接口配置命令。为了删除这个指定的访问组,使用 no 格式命令。

ip access-group {*access-list-name*}{**in** | **out**}

no ip access-group {access-list-name}{**in** | **out**}

参数

参数	参数说明
access-list-name	访问表名。这是一个最长为20个字符的字符串。
in	在进接口时使用访问列表。
out	在出接口时使用访问列表。

命令模式

接口配置态

使用说明

访问列表既可用在出接口也可用在入接口。对于标准的入口访问列表，在接收到包之后，对照访问列表检查包的源地址。对于扩展的访问列表，该路由器也检查目标地址。如果访问表允许该地址，那么软件继续处理该包。如果访问表不允许该地址，该软件放弃包并返回一个 ICMP 主机不可到达报文。

对于标准的出口访问表,在接收和路由一个包到控制接口以后，软件对照访问列表检查包的源地址。对于扩展的访问表，路由器还检查接收端访问表。如果访问表允许该软件就传送这个包。如果访问列表不允许该地址，软件放弃这个包并返回一个 ICMP 主机不可达报文。

如果指定的访问列表不存在，所有的包允许通过。

示例

下例在以太网接口 0 的包出口上应用列表 filter：

```
interface ethernet 0
ip access-group filter out
```

相关命令

ip access-list

show ip access-list

6.2.3 ip access-list

使用此命令后，进入的 IP 访问列表配置模式。在这状态下可以增加和删除访问规则。命令 exit 返回配置状态。

使用 no 前缀，删除 IP 访问列表。

ip access-list {**standard | extended**} *name*

no ip access-list {**standard | extended**} *name*

参数

参数	参数说明
standard	指定为标准访问列表
extended	指定为扩展访问列表
name	访问表名。这是一个最长20的字符串。

缺省

没有 IP 访问列表被定义。

命令模式

全局配置态

使用说明

使用此命令将进入 IP 访问列表配置模式，在 IP 访问列表配置模式中，可以用 deny 或 permit 命令来配置访问规则。

示例

以下的例子配置一个标准访问列表

```
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any
```

相关命令

deny

ip access-group

permit

show ip access-list

6.2.4 permit

在 IP 访问列表配置模式中可使用此命令配置允许规则，要从 IP 访问列表中删除 permit 规则，在命令前加 no 前缀。

permit source [*source-mask*] [**log**]

no permit source [*source-mask*] [**log**]

permit protocol source source-mask destination destination-mask [**precedence** *precedence*] [**tos** *tos*] [**log**]

no permit protocol source source-mask destination destination-mask [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于互联网控制报文协议(ICMP)，也可以使用以下句法:

permit icmp source source-mask destination destination-mask [**icmp-type**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于 Internet 组管理协议(IGMP)，可以使用以下句法:

permit igmp source source-mask destination destination-mask [**igmp-type**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于 TCP，可以使用以下句法:

permit tcp source source-mask [operator port] destination destination-mask [**operator** *port*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log**]

对于数据报协议(UDP)，可以使用以下句法:

permit udp source source-mask [**operator** *port* [*port*]] **destination destination-mask** [**operator** *port*] [**precedence** *precedence*] [**tos** *tos*] [**log**]

参数

参数	参数说明
protocol	协议名字或IP协议号。它可以是关键字icmp、igmp、igrp、ip、ospf、tcp或udp，也可以是表IP协议号的0到255的一个整数。为了匹配任何Internet协议(包括ICMP、TCP和UDP)使用关键字ip。某些协议允许进一步限定，如下描述。
source	源网络或主机号。有两种方法指定源：32位二进制数，用四个点隔开的十进制数表示。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
source-mask	源地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的源和源掩码缩写。
destination	目标网络或主机号。有两种方法指定： 使用四个点隔开的十进制数表示的32位二进制数。 使用关键字any作为0.0.0.0 0.0.0.0的目标和目标掩码的缩写。
destination-mask	目标地址网络掩码。使用关键字any作为0.0.0.0 0.0.0.0的目标地址和目标地址掩码缩写。
precedence precedence	(可选)包可以由优先级过滤，用0到7的数字指定。
tos tos	(可选) 数据包可以使用服务层过滤。使用数字0－15指定。
icmp-type	(可选)ICMP包可由ICMP报文类型过滤。类型是数字0到255。
igmp-type	(可选)IGMP包可由IGMP报文类型或报文名过滤。 类型是0到15的数字。
operator	(可选)比较源或目标端口。操作包括lt(小于)， gt(大于)，eq(等于)，neq(不等于)。如果操作符放在source和source-mask之后，那么它必须匹配这个源端口。如果操作符放在destination和destination-mask之后，那么它必须匹配目标端口。
port	(可选)TCP或UDP端口的十进制数字或名称。端口号是一个0到65535的数字。TCP端口名列在“使用方针”部分。当过滤TCP时，可以只使用TCP端

	口名称。UDP端口名称也列在“使用说明”部分。当过滤TCP时，只可使用TCP端口名。当过滤UDP时， 只可使用UDP端口名。
established	(可选)只对TCP协议，表示一个已建立的连接。如果TCP数据报ACK或RST位设置时，出现匹配。非匹配的情况是初始化TCP数据报，以形成一个连接。
log	(可选)可以进行日志记录。

命令模式

IP 访问列表配置态

使用说明

可以使用访问表控制包在接口上的传输，控制虚拟终端线路访问以及限制路由选择更新的内容。在匹配发生以后停止检查扩展的访问表。

分段 IP 包，而不是初始段，立即由任何扩展的 IP 访问表接收。扩展的访问表用于控制访问虚拟终端线路或限制路由选择更新的内容，不必匹配 TCP 源端口、服务值的类型或包的优先权。

注意：

在初始建立一个访问表后，任何后续的添加内容(可能由终端键入)放置在列表的尾部。

以下显示用于替换端口号的 TCP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个？替代端口号的方式来寻找。

- bgp
- ftp
- ftp-data
- login
- pop2
- pop3
- smtp
- telnet
- www

以下显示用于替换端口号的 UDP 端口名。参看当前的分配号 RFC 找到这些协议的有关参考。与这些协议相应的端口号也可以通过以键入一个？替代端口号的方式来寻找。

- domain
- snmp
- syslog
- tftp

示例

下面示例允许 192.168.5.0 这个网段：

```
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
```

注意：

IP 访问表由一个隐含的 deny 规则结束。

相关命令

deny

ip access-group

ip access-list

show ip access-list

6.2.5 ip http firewalltype

配置防火墙类型。

ip http firewalltype type

参数

参数	参数说明
type	类型。0:IP访问表由一个隐含的deny规则结束；1：IP访问表由一个隐含的permit规则结束。

缺省

默认 IP 访问表由一个隐含的 deny 规则结束。

命令模式

接口配置态

使用说明

配置防火墙类型。

注意：只在 web 页面配置 IP ACL 时生效

6.2.6 show ip access-list

要显示当前的 IP 访问列表内容，使用 show ip access-list 命令。

show ip access-list[*access-list-name*]

参数

参数	参数说明
access-list-name	访问表名。这是一个最长20的字符串。

缺省

显示所有标准的和扩展的 IP 访问列表。

命令模式

管理态

使用说明

show ip access-list 命令允许你指定一个特定的访问列表。

示例

以下是不指定名时 show ip access-list 命令的示例输出:

```
Router# show ip access-list
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

以下是指定访问表名时, show ip access-list 命令的示例输出:

```
ip access-list extended bbb
permit tcp any any eq www
permit ip any any
```

6.2.7 imp access-list

设置路由器 IP&MAC ACL。如果删除该 ACL，使用 no imp access-list 命令。

imp access-list <num>

no imp access-list <num>

参数

〈1-255〉

缺省

无

命令模式

全局配置态

使用说明

配置 IMP ACL 用于匹配 IP&MAC 地址的应用，比如 IP 地址和 MAC 地址进行绑定。

示例

下面的例子配置 IMP ACL：

Router_config#imp access-list 1

6.2.8 permit <ip | any> <mac | any>

设置路由器 IP&MAC ACL 的 permit 表项。如果删除 permit ACL 表项，使用 no permit <ip | any> <mac | any>命令。

permit <ip | any> <mac | any>

no permit <ip | any> <mac | any>

参数

ip 格式为 a.b.c.d,也可以为 any（即任意 ip 地址）；

mac 格式为 hh:hh:hh:hh:hh:hh，也可以为 any（即任意 mac 地址）。

缺省

无

命令模式

IMP ACL 配置模式

使用说明

配置 IMP ACL 的 permit 表项。

示例

下面的例子配置 IMP ACL 的 permit 表项：

Router_config_imp_acl#permit 1.1.1.1 00:a0:0c:13:64:7d

6.2.9 deny <ip | any> <mac | any>

设置路由器 IP&MAC ACL 的 deny 表项。如果删除 deny ACL 表项，使用 no deny <ip | any> <mac | any>命令。

deny <ip | any> <mac | any>

no deny <ip | any> <mac | any>

参数

ip 格式为 a.b.c.d,也可以为 any（即任意 ip 地址）；

mac 格式为 hh:hh:hh:hh:hh:hh，也可以为 any（即任意 mac 地址）。

缺省

无

命令模式

IMP ACL 配置模式

使用说明

配置 IMP ACL 的 deny 表项。

示例

下面的例子配置 IMP ACL 的 permit 表项：

Router_config_imp_acl#deny 1.1.1.2 00:a0:0c:13:64:7d

6.2.10 imp access-group

应用 IMP ACL。如果取消应用该 ACL，使用 no imp access-group 命令。

imp access-group <num>

no imp access-group <num>

参数

〈1-255〉

缺省

无

命令模式

端口配置态

使用说明

将配置的 IMP ACL 应用到实际端口上，以太网将解析 IP 报文，使用配置的 IMP ACL 进行过滤。

示例

下面的例子配置 IMP ACL：

Router_config_g0/0#imp access-group 1

6.2.11 Ip access-list extended *** massive

设置路由器采用特殊 acl 算法，加快 acl 查表的速度

ip access-list extended * massive**

no ip access-list extended *

参数

该命令没有参数或关键字

缺省

不启用特殊算法

命令模式

全局配置态

使用说明

在普通的扩展访问里表配置后增加massive关键字，即对该访问列表表项进行特殊算法处理,加快查表速度.

如果扩展访问列表里配置了 ip 地址范围的匹配或者 df 选项，那么算法不生效

标准访问列表不支持该算法.

示例

下面的例子启用快速转发功能：

Router_config#ip access-list extended test massive

Router_config_ext_nacl#permit ip 1.1.1.0 255.255.255.0 2.2.2.0 255.255.255.0

Router_config_ext_nacl#exit

Router_config#

Test 这个表项将启用算法，针对这个表里的每条规则查找都会采用算法来定位

6.2.12 Ip access-list table-limit ***

设置路由器采用特殊 acl 算法时， 设置每个算法表最多容纳多少 acl 规则

ip access-list table-limit ***

参数

<100-1000> ---rfc table limit

每个算法表最多容纳的 acl 规则数

缺省

默认没有上限， 所有当前配置的 acl 规则全部容纳在一个算法表里

命令模式

全局配置态

使用说明

因为算法内存消耗太大， 所以使用多个算法表， 分担 acl 规则， 会大幅减少内存消耗， 但性能也会明显下降

示例

Router_config#ip access-list table-limit 300

6.2.13 Ip access-list cache-enable

设置转发 cache 里加入 acl 查询结果

ip access-list cache-enable

参数

无

缺省

没有开启

命令模式

全局配置态

使用说明

示例

6.3 URPF配置命令

6.3.1 verify ipv4 unicast source reachable-via

在某个接口上开启 URPF 功能，有宽松和严格之分。为了关闭某个接口的 URPF 功能，使用 no 格式命令。

verify ipv4 unicast source reachable-via {**any** | **rx**} {allow-default} { access-list-name }

no verify ipv4 unicast source reachable-via {**any** | **rx**} {allow-default} { access-list-name }

参数

参数	参数说明
any	指定URPF为宽松的
rx	指定URPF为严格的
allow-default	表明URPF是否允许默认路由
access-list-name	当URPF失败时，可以通过配置ACL来指定例外

缺省

所有的接口上都不开启 URPF 功能

命令模式

接口配置态

使用说明

URPF（Unicast Reverse Path Forwarding，单播反向路径转发）的主要功能是用于防止基于源地址欺骗的网络攻击行为。源地址欺骗攻击为入侵者构造出一系列带有伪造源地址的报文，对于使用基于IP 地址验证的应用来说，此攻击方法可以导致未被授权用户以他人身份获得访问系统的权限，甚至是以管理员权限来访问。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。URPF 检查有严格（strict）型和松散（loose）型两种，严格意思是根据路由查到的出口必须跟报文进入的口一致，而宽松的意思是只要查到路由就可以了。如果没有配置allow-default,那么就会忽略默认路由。此外，还可以通过ACL 来指定例外，即URPF失败，但符合ACL规则的也能让报文通过。

注意：一定要在全局在开启verify ipv4 enable才能使接口上的URPF功能有效

示例

以下是在 G0/1 接口上配置宽松 URPF，并且允许默认路由:

```
!
interface GigaEthernet0/1
 Ip address 1.1.1.1 255.255.255.0
```

```
 verify ipv4 unicast source reachable-via any allow-default
!
```

以下是在 G0/0 接口上配置严格 URPF:

```
!
interface GigaEthernet0/1
 Ip address 1.1.1.1 255.255.255.0
 verify ipv4 unicast source reachable-via rx
!
```

6.4 ip fastswitch

设置路由器采用快速转发模式处理IPv4转发报文。如果要恢复默认模式，使用 no ip fastswitch命令。

ip fastswitch [*number*]

no ip fastswitch

参数

number 系统接收缓存队列的长度，可以通过该值来调整系统接收缓冲队列的长度，从而影响转发时延。

缺省

不启用快速转发模式

命令模式

全局配置态

使用说明

启用快速转发模式后，某些业务的处理能力将得到提升，如IPv4转发、IPACL、NAT等，但有些业务的处理能力并不会改变，如IPSec等。

示例

下面的例子启用快速转发功能，并设置系统接收缓冲队列长度为1024：

```
Router_config#ip fastswitch 1024
```

6.5 FTP配置命令

6.5.1 ftp-server enable

设置路由器启用 ftp 服务器。如果要恢复默认模式，使用 no ftp-server enable 命令。

ftp-server enable

no ftp-server enable

参数

该命令没有参数或关键字

缺省

不启用 ftp 服务器

命令模式

全局配置态

使用说明

启用 ftp 服务器后，路由器在 21 端口侦听 ftp 客户端(IPv4、IPv6)，如果 ftp-server certificate 同时配置的话，也在 990 端口侦听隐式 ftp over SSL/TLS 客户端(详见 1.6)。

示例

下面的例子启用 ftp 服务器：

Router_config#ftp-server enable

6.5.2 ftp-server maxlogin

设置路由器 ftp 服务器最大用户同时登录数。如果要恢复默认模式，使用 no ftp-server maxlogin 命令。

ftp-server maxlogin *maxlogin*

no ftp-server maxlogin

参数

参数	参数说明
maxlogin	设置的最大用户同时登录数，范围为<1-1024>

缺省

ftp 服务器最大登录连接数无限制

命令模式

全局配置态

使用说明

启用 ftp 服务器并配置最大用户同时登录数后，若已连接的 ftp 会话小于这个数目，再连接之后的会话连接至多是这个数目；若已连接的 ftp 会话达到或者超过这个数目，系统将不再接受 ftp 连接。

示例

下面的例子配置最大用户同时登录数为 5：

Router_config#ftp-server maxlogin 5

6.5.3 ftp-server attack-defense

设置路由器启用 ftp 服务器攻击防护检测。如果要恢复默认模式，使用 ftp-server attack-defense 命令。

ftp-server attack-defense

no ftp-server attack-defense

参数

该命令没有参数或关键字

缺省

启用 ftp 服务器攻击防护检测

命令模式

全局配置态

使用说明

启用 ftp 服务器并配置攻击防护检测后，如果 60 秒内 ftp 客户端有 5 次用户名和密码的错误输入，ftp 服务器将启用静默模式，此后的 60 秒内不要接受新的连接。

命令不可与 ftp-server anonymous-permission 同时使用。

示例

下面的例子启用 ftp 服务器攻击防护检测：

Router_config#ftp-server attack-defense

6.5.4 ftp-server anonymous-permission

设置路由器启用 ftp 服务器允许匿名登录。如果要恢复默认模式，使用 no ftp-server anonymous-permission 命令。

ftp-server anonymous-permission

no ftp-server anonymous-permission

参数

该命令没有参数或关键字

缺省

ftp 服务器不允许匿名登录

命令模式

全局配置态

使用说明

启用 ftp 服务器并配置允许匿名登录后，ftp 客户端可以匿名方式以任意用户名和密码登录到 ftp 服务器。

命令不可与 ftp-server attack-defense 同时使用。

示例

下面的例子启用 ftp 服务器攻击防护检测：

Router_config#ftp-server attack-defense

6.5.5 ftp-server certificate

设置路由器 ftp 服务器 FTP over SSL/TLS 的认证证书文件。如果要恢复默认模式，使用 no ftp-server certificate 命令。

ftp-server certificate *filename*

no ftp-server certificate

参数

参数	参数说明
filename	设置FTP over SSL/TLS的认证证书文件名

缺省

不配置 FTP over SSL/TLS 的认证证书文件

命令模式

全局配置态

使用说明

配置 FTP over SSL/TLS 的认证证书文件后，如果文件为正确的认证文件，再配置启用 ftp 服务器的命令，ftp 客户端可以 FTP over SSL/TLS 的方式登录到路由器 990 端口下的 ftps 服务器。

命令不负责验证文件的正确性，若之后配置 ftp-enable 提示“FTP over SSL/TLS socket listen failure”，请重新配置。

示例

下面的例子设置路由器 ftp 服务器 FTP over SSL/TLS 的认证证书文件,并启用 ftps：

Router_config#ftp-server certificate cert.crt

Router_config#ftp-server enable

6.5.6 ftp-server user-group

设置路由器 ftp 服务器用户组。

ftp-server user-group *groupname*

no ftp-server user-group *groupname*

参数

参数	参数说明
groupname	设置FTP用户组

缺省

命令模式

全局配置态

使用说明

配置用户组，进入 ftp 服务器用户组配置态，可以添加删除用户名及密码，设置组权限。

删除用户组，同时会将组下所有用户名及密码删除

示例

下面的例子设置 ftp 服务器用户组：

Router_config#ftp-server usergroup grp1

Router_config_ftpd_usergroup#

6.5.7 ftp-user

设置路由器 ftp 服务器用户组。

ftp-user *username* **password** *password*

no ftp-user *username*

参数

参数	参数说明
username	设置FTP登录用户名
password	设置FTP登录密码

缺省

命令模式

ftp 服务器用户组配置态

使用说明

在 ftp 服务器用户组配置态下，添加或删除 FTP 登录用户名及密码

示例

下面的例子设置 ftp 服务器用户组：

Router_config_ftpd_usergroup#ftp-user usr1 password pas1

6.5.8 privilege

设置路由器 ftp 服务器用户组权限。如果要恢复默认模式，使用 privilege read 命令。

privilege [read | write | execute]

参数

参数	参数说明
username	设置FTP登录用户名
password	设置FTP登录密码

缺省

给用户组读权限

命令模式

ftp 服务器用户组配置态

使用说明

在 ftp 服务器用户组配置态下，修改用户组的读写执行权限。

读权限：下载文件。

写权限：上传文件(服务器上无同名文件，若有同名文件，还需要执行权限)

执行权限：删除文件/文件夹，重命名文件(不支持重命名文件夹)，创建/删除文件夹。

注：不支持中文文件名。

示例

下面的例子设置 ftp 服务器用户组的权限包括读写执行：

Router_config_ftpd_usergroup# privilege read write execute

6.6 防攻击配置命令

6.6.1 verify ipv4 enable

开启或关闭防攻击功能

verify ipv4 enable

no verify ipv4 enable

参数

该命令没有参数或关键字

缺省

不开启防攻击功能

命令模式

全局配置态

使用说明

防攻击功能开启后，可以保护主机免于攻击，现在主要支持的防攻击有：ping flood 攻击，ping 扫描攻击，syn flood 攻击，syn 端口扫描攻击，fin 端口扫描攻击，rst flood 攻击，udp flood 攻击，udp 端口扫描攻击，ping of death， teardrop 攻击等

示例

以下是开启防攻击功能的配置：

!

verify ipv4 enable

1.1.2 verify ipv4 log-enable

开启或关闭防攻击日志告警功能

verify ipv4 log-enable

no verify ipv4 log-enable

参数

该命令没有参数或关键字

缺省

不开启防攻击日志告警功能

命令模式

全局配置态

使用说明

防攻击日志告警功能开启后，当某台主机被探测到受到攻击时，会相应地输出日志告警信息

示例

以下是开启防攻击日志告警功能的配置：

!

verify ipv4 log-enable

6.6.2 verify ipv4 filter

开启或关闭防攻击报文过滤功能

verify ipv4 filter

no verify ipv4 filter

参数

该命令没有参数或关键字

缺省

不开启防攻报文过滤功能

命令模式

全局配置态

使用说明

防攻击报文过滤功能开启后，当某台主机被探测到受到攻击时，会将相应的报文丢弃，比如当探测到 syn flood 攻击，只有超过阀值的报文才被丢弃，而开启报文过滤功能后，只要探测到是 syn flood 攻击后，所有相应的报文都将被丢弃

示例

以下是开启防攻击报文过滤功能的配置：

!

verify ipv4 filter

6.6.3 verify ipv4 all

开启或关闭所有支持的防攻击功能

verify ipv4 all

no verify ipv4 all

参数

该命令没有参数或关键字

缺省

不开启所有的防攻击功能

命令模式

全局配置态

使用说明

用该命令开启或关闭所有支持防攻击功能，无需一条条地去打开或关闭

6.6.4 verify ipv4 icmp

开启防 ping flood 攻击和 ping 扫描攻击功能

verify ipv4 icmp {ping-flood| ping-sweep} [*value*]

no verify ipv4 icmp {ping-flood| ping-sweep} [*value*]

参数

参数	参数说明
ping-flood	开启防 ping flood 攻击
ping-sweep	开启防 ping 扫描攻击
value	配置相关的参数 缺省

不开启防 ping flood 和 ping 扫描攻击功能

命令模式

全局配置态

使用说明

对于防 ping flood 攻击功能，可配置相应的阀值，限制某台主机一秒内收到的 ping 报文数，默认为 300。对于防 ping 扫描攻击，可以配置相应的时间，在该时间内 ping 扫描的不同地址数达到 32 个，则认为是 ping 扫描攻击，默认是 3 秒

示例

以下是开启防 ping flood 和 ping 扫描攻击的配置：

```
!
verify ipv4 icmp ping-flood 300
verify ipv4 icmp ping-sweep 3
```

1.1.6 verify ipv4 tcp

开启防 syn flood、syn 端口扫描、fin 端口扫描和 rst flood 攻击功能

verify ipv4 tcp {syn-flood| syn-sweep|fin-scan|rst-flood} [*value*]

no verify ipv4 tcp {syn-flood| syn-sweep|fin-scan|rst-flood} [*value*]

参数

参数参数说明

syn-flood	开启防 syn flood 攻击
syn-sweep	开启防 syn 端口扫描攻击
fin-scan	开启防 fin 端口扫描攻击
rst-flood	开启防 rst flood 攻击
value	配置相关的参数 **缺省**

不开启相应的防攻击功能

命令模式

全局配置态

使用说明

对于防 syn flood 攻击功能，可配置相应的阀值，限制某台主机一秒内收到的 syn 报文数，默认为 300。对于防 syn 端口扫描攻击，可以配置相应的时间，在该时间内 syn 扫描的不同端口数达到 32 个，则认为是 syn 端口扫描攻击，默认是 3 秒。对于防 fin 端口扫描攻击，可以配置相应的时间，在该时间内 fin 扫描的不同端口数达到 32 个，则认为是 fin 端口扫描攻击，默认是 3 秒。对于防 rst flood 攻击功能，可配置相应的阀值，限制某台主机一秒内收到的 rst 报文数，默认为 300。

示例

以下是开启防 syn flood、syn 端口扫描、fin 端口扫描和 rst flood 攻击功能的配置：

```
!
verify ipv4 tcp syn-flood 300
verify ipv4 tcp syn-sweep 3
verify ipv4 tcp fin-scan 3
verify ipv4 tcp rst-flood 300
```

1.1.7 verify ipv4 udp

开启防 udp flood 和 udp 端口扫描攻击功能

verify ipv4 udp {udp-flood| udp-sweep } [*value*]

no verify ipv4 udp {udp-flood| udp-sweep } [*value*]

参数

参数参数说明

udp-flood	开启防 udp flood 攻击
udp-sweep	开启防 udp 端口扫描攻击
value	配置相关的参数 **缺省**

不开启相应的防攻击功能

命令模式

全局配置态

使用说明

对于防 udp flood 攻击功能，可配置相应的阀值，限制某台主机一秒内收到的 udp 报文数，默认为 300。对于防 udp 端口扫描攻击，可以配置相应的时间，在该时间内 udp 扫描的不同端口数达到 32 个，则认为是 udp 端口扫描攻击，默认是 3 秒。

示例

以下是开启防 udp flood 和 udp 端口扫描攻击功能的配置：

```
!
verify ipv4 udp udp-flood 300
verify ipv4 udp udp-sweep 3
```

1.1.8 verify ipv4 attack

开启防 xmas-tree, null-scan, land, smurf, winnuke, ping of death, teardrop, fraggle 攻击功能

verify ipv4 attack
{xmas-tree|null-scan|land|smurf|winnuke|ping-of-death|teardrop|fraggle} [*value***]**

no verify ipv4 attack
{xmas-tree|null-scan|land|smurf|winnuke|ping-of-death|teardrop|fraggle} [*value***]**

参数

参数参数说明

xmas-tree	开启防 xmas-tree 攻击

null-scan	开启防 null scan 攻击
land	开启防 land 攻击
smurf	开启防 smurf 攻击
winnuke	开启防 winnuke 攻击
ping-of-death	开启防 ping of death 攻击
teardrop	开启防 teardrop 攻击
fraggle	开启防 fraggle 攻击
value	配置相关的参数 **缺省**

不开启相应的防攻击功能

命令模式

全局配置态

使用说明

对于防 xmas-tree 攻击功能可以配置相应的时间，在该时间内收到同时置上了 FIN ，PUSH 和 URG 的 TCP 报文扫描的不同端口数达到 32 个，则认为是 xmas-tree 攻击，默认是 3 秒。对于防 null-scan 攻击功能可以配置相应的时间，在该时间内收到同时置上了 tcp 标志为 0 的 TCP 报文扫描的不同端口数达到 32 个，则认为是 null-scan 攻击，默认是 3 秒。

示例

以下是开启防 xmas-tree, null-scan, land, smurf, winnuke, ping of death, teardrop, fraggle 攻击功能的配置：

```
!
verify ipv4 attack Xmas-Tree 3
verify ipv4 attack Null-scan 3
verify ipv4 attack Land
verify ipv4 attack Smurf
verify ipv4 attack WinNuke
verify ipv4 attack Ping-of-Death
verify ipv4 attack TearDrop
verify ipv4 attack Fraggle
```

6.7 报文连续处理个数配置命令

6.7.1 packet-handle-pause

配置报文连续处理个数，每处理指定个数个报文暂停一下，让别的处理流程运行。

packet-handle-pause per *number*

no packet-handle-pause

参数

参数	参数说明
number	报文连续处理个数

缺省

默认报文连续处理个数为 100 个

命令模式

全局配置态

使用说明

用于配置报文连续处理的个数，从而调节报文处理的性能。执行 no packet-handle-pause 后，在等待处理的报文队列里存在报文的情况下，报文处理始终连续进行，直到等待处理队列为空。

示例

以下是配置报文连续个数的例子：

!

packet-handle-pause per 500

6.8 硬件优先接收匹配模式配置命令

6.8.1 cavium pip-watcher

利用硬件功能，设定报文匹配规则，以确保一些路由协议报文能够被硬件优先接收。

cavium pip-watcher *match-type match-value*

no cavium pip-watcher *match-type match-value*

参数

参数	参数说明
match-type	<0 - 4>，硬件优先接收的匹配类型。0 为关闭匹配，1 为 IP 协议字段，2 为 TCP 目的端口号，3 为 UDP 目的端口号，5 为以太网协议字段
match-value	匹配值

缺省

无

命令模式

全局配置态

使用说明

一般针对路由协议的协议报文，如 BGP、OSPF、ISIS 等。

示例

下面的这条命令将确保 ospf 的协议报文能够被优先接收。

cavium pip-watcher 1 0x59

相关命令

show cavium pip-watcher

6.9 系统MTU配置命令

6.9.1 System mtu

设定系统可以接收的报文最大长度。

system mtu *max-frame-size*

no system mtu

参数

参数	参数说明
max-frame-size	<64 - 60000>，硬件可接收的最大长度，单位为byte

缺省

无

命令模式

全局配置态

使用说明

无

示例

下面的这条命令将使硬件能够接收 64-1500 长度区间内的报文。

system mtu 1500

相关命令

无