

目 录

第 1 章 L3 转发配置命令	1-1
1.1 三层接口配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 description	1-1
1.1.3 description (VRF配置模式)	1-1
1.1.4 interface vlan	1-2
1.1.5 interface loopback	1-2
1.1.6 ip vrf	1-3
1.1.7 ip vrf forwarding vrfName	1-3
1.1.8 no interface IFNAME	1-3
1.1.9 rd	1-4
1.1.10 route-target	1-4
1.1.11 show ip route vrf	1-5
1.1.12 show ip vrf	1-5
1.1.13 shutdown	1-6
1.2 IP(v4/v6)配置基本命令	1-6
1.2.1 clear ip traffic	1-6
1.2.2 clear ipv6 neighbor	1-6
1.2.3 debug ip icmp	1-7
1.2.4 debug ip packet	1-7
1.2.5 debug ipv6 packet	1-8
1.2.6 debug ipv6 icmp	1-8
1.2.7 debug ipv6 nd	1-9
1.2.8 debug ipv6 tunnel packet	1-9
1.2.9 description	1-10
1.2.10 ipv6 proxy enable	1-10
1.2.11 ip address	1-10
1.2.12 ipv6 address	1-10
1.2.13 ipv6 route	1-11
1.2.14 ipv6 redirect	1-11
1.2.15 ipv6 nd dad attempts	1-12
1.2.16 ipv6 nd ns-interval	1-12
1.2.17 ipv6 nd suppress-ra	1-12
1.2.18 ipv6 nd ra-lifetime	1-13
1.2.19 ipv6 nd min-ra-interval	1-13
1.2.20 ipv6 nd max-ra-interval	1-13
1.2.21 ipv6 nd prefix	1-14
1.2.22 ipv6 nd ra-hoplimit	1-14

1.2.23 ipv6 nd ra-mtu	1-14
1.2.24 ipv6 nd reachable-time	1-15
1.2.25 ipv6 nd retrans-timer	1-15
1.2.26 ipv6 nd other-config-flag	1-15
1.2.27 ipv6 nd managed-config-flag	1-15
1.2.28 ipv6 neighbor	1-16
1.2.29 interface tunnel	1-16
1.2.30 show ip interface	1-17
1.2.31 show ip traffic	1-17
1.2.32 show ipv6 interface	1-19
1.2.33 show ipv6 route	1-20
1.2.34 show ipv6 neighbors	1-21
1.2.35 show ipv6 traffic	1-22
1.2.36 show ipv6 redirect	1-23
1.2.37 show ipv6 tunnel	1-23
1.2.38 tunnel source	1-24
1.2.39 tunnel destination	1-24
1.2.40 tunnel nexthop	1-24
1.2.41 tunnel 6to4-relay	1-25
1.2.42 tunnel mode	1-25
1.3 网管端口配置命令	1-25
1.3.1 duplex	1-25
1.3.2 interface ethernet	1-25
1.3.3 ip address	1-26
1.3.4 shutdown	1-26
1.3.5 speed	1-26
1.4 IP路由聚合配置命令	1-26
1.4.1 ip fib optimize	1-26
1.5 URPF命令	1-27
1.5.1 debug urpf	1-27
1.5.2 ip urpf enable	1-27
1.5.3 show urpf rule ipv4 num	1-28
1.5.4 show urpf rule ipv6 num	1-28
1.5.5 show urpf rule ipv4	1-28
1.5.6 show urpf rule ipv6	1-29
1.5.7 show urpf	1-29
1.5.8 urpf enable	1-29
1.6 ARP转发配置命令	1-29
1.6.1 arp	1-29
1.6.2 clear arp-cache	1-30
1.6.3 clear arp traffic	1-30

1.6.4 debug arp	1-30
1.6.5 ip proxy-arp	1-31
1.6.6 l3 hashselect.....	1-31
1.6.7 show arp.....	1-32
1.6.8 show arp traffic	1-32
1.7 l3 station movement配置命令	1-33
1.7.1 l3-station-move.....	1-33
第 2 章 防ARP扫描功能命令	2-1
2.1 anti-arpscan enable [ip port].....	2-1
2.2 anti-arpscan port-based threshold.....	2-1
2.3 anti-arpscan ip-based level1 level2 threshold.....	2-1
2.4 anti-arpscan trust	2-2
2.5 anti-arpscan trust ip	2-2
2.6 anti-arpscan recovery enable	2-2
2.7 anti-arpscan recovery time	2-3
2.8 anti-arpscan log enable.....	2-3
2.9 anti-arpscan trap enable [level1 level2]	2-3
2.10 anti-arpscan ip-based level2 action {isolate discard-ARP}.....	2-4
2.11 anti-arpscan FFP max-num <num>	2-4
2.12 anti-arpscan ip-based arp-to-cpu speed<pps>	2-4
2.13 show anti-arpscan	2-4
2.14 show anti-arpscan ip-based attack-list [history].....	2-6
2.15 show anti-arpscan ip-based running-config	2-7
2.16 clear anti-arpscan speed-limit< IP Address>.....	2-7
2.17 clear anti-arpscan ip-isolate <IP Address>.....	2-7
2.18 clear anti-arpscan attack-list {ip <IP Address> all}.....	2-7
2.19 clear anti-arpscan attack-history-list {ip <IP Address> all}.....	2-8
2.20 debug anti-arpscan.....	2-8
第 3 章 ARP、ND绑定配置命令	3-1
3.1 ip arp-security updateprotect	3-1
3.2 ipv6 nd-security updateprotect	3-1
3.3 ip arp-security learnprotect	3-1

3.4 ipv6 nd-security learnprotect.....	3-2
3.5 ip arp-security convert	3-2
3.6 ipv6 nd-security convert	3-2
3.7 clear ip arp dynamic	3-3
3.8 clear ipv6 nd dynamic	3-3
第 4 章 ARP GUARD配置命令	4-1
4.1 arp-guard ip.....	4-1
第 5 章 Arp local proxy命令	5-1
5.1 ip local proxy-arp.....	5-1
第 6 章 免费ARP发送功能配置命令	6-1
6.1 ip gratuitous-arp	6-1
6.2 show ip gratuitous-arp	6-1
第 7 章 Keepalive gateway配置命令.....	7-1
7.1 keepalive gateway	7-1
7.2 show ip interface	7-1
7.3 show keepalive gateway	7-1
第 8 章 UFT配置命令	8-1
8.1 Show system working mode	8-1
8.2 System working mode.....	8-1

第1章 L3 转发配置命令

1.1 三层接口配置命令

1.1.1 bandwidth

命令: **bandwidth <bandwidth>**
no bandwidth

功能: 配置 interface vlan 的带宽。本命令的 no 命令为恢复 interface vlan 的带宽值为默认值。

interface vlan 接口下面的 bandwidth 不会实际控制端口的带宽, 而是用于协议计算。例如, OSPF 计算链路的 cost 时, 使用的就是接口的 bandwidth ($\text{cost} = 10^8 / \text{bandwidth}$), 因此改变 bandwidth 会导致 OSPF 链路 cost 的改变。

参数: **<bandwidth>**: interface vlan 带宽值。范围<1-10000000000 bits>。可取的单位有 k, m, g。该值转化 bit 后不能有小数。

命令模式: VLAN 接口配置模式。

缺省情况: interface vlan 默认带宽值为 100,000,000bit。

使用指南: 该命令只能应用于 interface vlan 接口。本命令单位换算关系: 1g=1,000m=1,000,000k=1,000,000,000bit。

举例: 配置 vlan 1 的带宽值为 50,000,000bit。

Switch(Config-if-Vlan1)#bandwidth 50m

1.1.2 description

命令: **description <text>**
no description

功能: 配置 VLAN 接口的描述信息; 其 no 形式取消该 VLAN 接口的描述信息。

参数: **<text>**为 VLAN 接口的描述信息, 它的长度不超过 256 的字符串。

命令模式: VLAN 接口配置模式

缺省情况: 默认不配置。

使用指南: description 后面为用户对 VLAN 接口的描述信息, 会显示在所配置的 VLAN 下。

举例: 配置 VLAN 接口的描述信息为 test vlan。

Switch(config)#interface vlan 2

Switch(config-if-vlan2)#description test vlan

1.1.3 description (VRF配置模式)

命令: **description <text>**
no description

功能: 配置 VRF 的描述信息, 可用来记录 VPN 实例与某个 VPN 的关系等信息; 其 no 形

式取消该 VPN 的描述信息。

参数：**<text>**：描述性文本，1-256 个字符。

缺省情况：默认不配置。

命令模式：VRF 配置模式。

使用指南：description 后面为用户对 VRF 的描述信息。会显示在所配置的 VRF 下，以提供相关的指示信息。

举例：配置 VRF 的描述信息为“associate with VRF-B VRF-C”

```
Switch(config)#ip vrf VRF-A
```

```
Switch(config-vrf)#description associate with VRF-B VRF-C
```

1.1.4 interface vlan

命令：interface vlan <vlan-id>

no interface vlan <vlan-id>

功能：创建一个 VLAN 接口，即创建一个交换机的三层接口；本命令的 no 操作为删除交换机指定的三层接口。

参数：**<vlan-id>** 是已建立的 VLAN 的 VLAN ID，取值范围 1~4094。

缺省情况：出厂时没有三层接口。

命令模式：全局配置模式。

使用指南：在创建 VLAN 接口（三层接口）前，需要先配置 VLAN。使用本命令在创建 VLAN 接口（三层接口）的同时，进入 VLAN 接口（三层接口）配置模式。在 VLAN 接口（三层接口）创建好之后，仍旧可以使用 interface vlan 命令进入三层接口模式。使用命令 **exit** 可以从 VLAN 接口配置模式退回到全局配置模式。

举例：在 VLAN 1 上创建一个 VLAN 接口（三层接口）。

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#
```

1.1.5 interface loopback

命令：interface loopback <loopback -id>

no interface loopback <loopback -id>

功能：创建一个 Loopback 接口；本命令的 no 操作为删除指定的 Loopback 接口。

参数：**<loopback-id>** 是已建立的 Loopback 的 ID。

缺省情况：出厂时没有 Loopback 接口。

命令模式：全局配置模式。

使用指南：配置的 Loopback 接口其实占用了 ID 从 1006 开始的 VLAN。若 Loopback 占用了 VLAN 1006 以后(包括 VLAN 1006)的某个 VLAN，则不能再配置对应的 VLAN；若原先已配置某 VLAN 1006 后的某个 VLAN，比如 VLAN 1006，则配置的 Loopback 接口占用其后第一个未被占用的 VLAN，比如 VLAN 1007。

举例：进入 Loopback 1 接口配置模式。

```
Switch(config)#interface loopback 1
```

```
Switch(Config-if-Loopback1)#
```

1.1.6 ip vrf

命令： ip vrf <vrf-name>

no ip vrf <vrf-name>

功能： 配置相应名称的 VPN 实例；其 no 形式取消该 VPN 实例。

参数： <vrf-name>：配置的 VPN 实例名称，取值长度范围 1~64。

缺省情况： 默认不配置。

命令模式： 全局配置模式。

使用指南： 配置相应名称的 VPN 实例。PE 上没有缺省的 VPN 实例，一个 PE 上可以创建多个 VPN 实例。VPN 实例的名字区分大小写。需要注意：VPN 实例只有配置了 RD 后才生效。

举例：

```
Switch(config)#ip vrf VRF-A
```

```
Switch(config-vrf)#
```

1.1.7 ip vrf forwarding vrfName

命令： ip vrf forwarding <vrfName> [fallback global]

no ip vrf forwarding <vrfName> [fallback global]

功能： 关联接口到指定 VRF。设定接口 fallback global 选项，如果接口作为 IP 报文入接口，在其绑定的 VRF 的路由表查找失败，可以跳转到全局路由表进行二次查找。

参数： <vrfName> 为 VRF 名称，它是一个长度小于 32 的字符串；

fallback global： 查询全局路由表。指定了 fallback global 选项以后，如果在接口绑定的 VRF 的路由表查找失败，可以跳转到全局路由表进行二次查找。

缺省情况： 系统默认将接口绑定于主 VRF。

命令模式： 接口配置模式。

使用指南： 如果该接口有访问 Internet 的需求，可以配置此命令。一个接口只能绑定到一个 VRF，一个 VRF 可以绑定多个接口。支持 VPN 的 IGP 记录端口和 VRF 之间的绑定关系，从绑定端口接收到路由，就加入与之绑定的 VRF 路由表。默认情况下，接口不关联任何 VRF，属于公网接口。

举例：

```
Switch(config)#int vlan 9
```

```
Switch(Config-if-Vlan9)#ip vrf forwarding vpn1 fallback global
```

1.1.8 no interface IFNAME

命令： no interface IFNAME

功能： 删除 interface 接口，只处理 interface vlan 和 interface loopback 两种接口。

参数：IFNAME：接口名。

命令模式：全局模式。

使用指南：该命令用以删除三层接口，是处理接口名是特殊拼写形式的情况。IFNAME 可以匹配多种形式的拼写，如 vlan1、Vlan1、v1、V1 等。

举例：删除 interface vlan1 这个接口。

```
(config)# no interface vlan1
```

1.1.9 rd

命令：rd <ASN:nn_or_IP-address:nn>

功能：配置 VRF 的 RD（Route Distinguish）。

参数：ASN:nn_or_IP-address:nn：路由器标识的 IP 地址格式。

缺省情况：默认不配置。

命令模式：VRF 配置模式。

使用指南：RD 用于对 VPN 路由进行唯一标识，VPN 实例通过 RD 实现地址空间独立，可以实现不同 VPN 之间的地址重叠。通常设置由 AS 号和一个任意数组成。无法直接删除 RD。

举例：

```
Switch (config)#ip vrf VRF-A
```

```
Switch (config-vrf)# rd 300:3
```

```
Switch (config-vrf)#
```

1.1.10 route-target

命令：route-target {import | export | both} <rt-value>

no route-target {import | export | both} <rt-value>

功能：配置指定 VRF 的 Route-Target；no 命令删除配置。

参数：**import：**表示对路由进行入口过滤，即判断 VPN 路由是否可以加入本 VRF；

export：表示当将本 VRF 的路由作为 VPNv4 路由向外发送时需附加的 Route-Target，用于对端口进行入口过滤；

both：表示 import、export 使用相同的 Route-Target 值；

<rt-value>：表示路由目标值。

缺省情况：默认不配置。

命令模式：VRF 配置模式。

使用指南：一个 RT 是一个 BGP 扩展团体，用于对 VPN 路由进行过滤，实现对直连 site 的 VPN 成员关系和路由规则的控制。对于配置的 import 规则，遍历所有 BGP 进程收到的路由，对符合条件的路由（路由的 export route-target 与本 VRF 的 import route-target 有交集），添加到该 VRF 下的 BGP 进程中，并向该 VRF 下的 BGP 私网邻居发布路由更新消息。对于配置的 export 规则，遍历该 VRF 关联的 BGP 进程中存储的所有 BGP 路由，对这些路由增加一个 export route-target，之后向所有公网邻居发布路由更新消息，同时，如果有其它

VRF 的 import route-target 与该 export route-target 相匹配，则复制一份路由到匹配 VRF 中，并向这个 VRF 下的 BGP 私网邻居发布路由更新。

举例：

```
Switch (config)#ip vrf VRF-A
Switch (config-vrf)# route-target both 100:1
Switch (config-vrf)#
```

1.1.11 show ip route vrf

命令：show ip route vrf <vrf-name> [bgp | database]

参数：<vrf-name>：VRF 名称，通过 if vrf <vrf-name>命令创建；

bgp：表示通过 BGP 引入的路由；

database：IP 路由表数据库。

缺省情况：无。

命令模式：任意配置模式。

使用指南：可以针对指定的路由协议显示。

举例：

```
Switch#show ip route vrf vrf-a bgp
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:10 (Default for VRF test)
*> 11.1.1.0/24 11.1.1.64 0 0 200 ?
*> 20.1.1.0/24 11.1.1.64 0 0 200 ?
```

1.1.12 show ip vrf

命令：show ip vrf [<vrf-name>]

功能：本命令显示与该 VPN 路由/转发实例相关的 RIP 实例信息。可显示绑定 VRF 的接口配置 fallback global 选项。

参数：<vrf-name>指明了 VPN 路由/转发实例的名称。

缺省情况：缺省不显示。

命令模式：任意模式。

使用指南：本命令在其它的路由协议中也存在，使用本命令时，与该 VPN 路由/转发实例相关的其它路由协议进程的信息也会显示出来。

举例：显示与 IPI 的 VRF 路由/转发实例相关的 RIP 实例信息。

```
Switch# show ip vrf IPI
VRF IPI, FIB ID 1
Router ID: 11.1.1.1 (automatic)
Interfaces:
Vlan1
```

```
!
VRF IPI; (id=1); RIP enabled Interfaces:
Ethernet1/8
```

Name	Interfaces
IPI	Vlan1

Name	Default RD	Interfaces
IPI		Vlan1

1.1.13 shutdown

命令： shutdown
no shutdown

功能： 关闭交换机的指定 VLAN 接口；本命令的 no 操作为打开 VLAN 接口。

命令模式： VLAN 接口配置模式。

缺省情况： VLAN 接口缺省为打开。

使用指南： 当关闭交换机的 VLAN 接口，VLAN 接口将不发送数据帧。如果交换机的 VLAN 接口需要通过 BOOTP/DHCP 协议获取 IP 地址时，必须将 VLAN 接口打开。

举例： 打开交换机的 VLAN1 接口。

```
Switch(Config-if-Vlan1)#no shutdown
```

1.2 IP(v4/v6)配置基本命令

1.2.1 clear ip traffic

命令： clear ip traffic

功能： 清除 IP 协议统计信息。

参数： 无。

缺省情况： 无。

命令模式： 特权用户配置模式。

使用指南： 清除 IP 内核协议收发数据包的统计信息，包括 IP 协议，ICMP 协议、TCP 协议和 UDP 协议的收包统计、发包统计、丢包统计以及收发数据包的错误信息等内容。

举例： 清除 ip 协议统计信息

```
Switch#clear ip traffic
```

1.2.2 clear ipv6 neighbor

命令： clear ipv6 neighbors

功能： 清除 IPv6 的邻居缓存。

参数：无。

命令模式：特权配置模式。

缺省情况：无。

使用指南：该命令不能清除静态邻居。

举例：清除邻居表。

Switch #clear ipv6 neighbors

1.2.3 debug ip icmp

命令：debug ip icmp

no debug ip icmp

功能：ICMP 数据包收发调试信息。

参数：无。

缺省情况：无。

命令模式：特权用户配置模式。

使用指南：

举例：

Switch#debug ip icmp

IP ICMP: sent, type 8, src 0.0.0.0, dst 20.1.1.1

显示内容	解释
IP ICMP: sent	发送 ICMP 数据报
type 8	类型为 8（PING 请求）
src 0.0.0.0	源 IPv4 地址
dst 20.1.1.1	目的 IPv4 地址

1.2.4 debug ip packet

命令：debug ip packet

no debug ip packet

功能：打开 IP 报文调试开关；本命令的 no 操作为关闭调试开关。

参数：无。

缺省情况：缺省 IP 数据包调试功能是关闭的。

命令模式：特权用户配置模式。

使用指南：显示接收或发送的 IP 数据包的内容，包括：源地址、目的地址、字节数等。

举例：打开 IP 报文调试开关。

Switch #debug ip packet

IP PACKET: sent, src 200.1.1.35, dst 224.0.0.9, size 312, proto 17, vrf 0

IP PACKET: rcvd, src 101.1.1.1, dst 224.0.0.9, size 312, proto 17, from Vlan200, vrf 0

1.2.5 debug ipv6 packet

命令：debug ipv6 packet

no debug ipv6 packet

功能：IPv6 数据包收发调试信息。

参数：无。

缺省情况：无。

命令模式：特权模式。

使用指南：

举例：

Switch#debug ipv6 packet

IPv6 PACKET: rcvd, src <fe80::203:fff:fe01:2786>, dst <fe80::1>, size <64>, proto <58>, from Vlan1

显示内容	解释
IPv6 PACKET: rcvd	接收 IPv6 数据报
src <fe80::203:fff:fe01:2786>	源 IPv6 地址
dst <fe80::1>	目的 IPv6 地址
size <64>	数据报的大小
proto <58>	IPv6 头中协议字段
from Vlan1	IPv6 数据报是从三层口 vlan 1 收上来

1.2.6 debug ipv6 icmp

命令：debug ipv6 icmp

no debug ipv6 icmp

功能：ICMP 数据包收发调试信息。

参数：无。

缺省情况：无。

命令模式：特权模式。

使用指南：

举例：

Switch#debug ipv6 icmp

IPv6 ICMP: sent, type <129>, src <2003::1>, dst <2003::20a:ebff:fe26:8a49> from Vlan1

显示内容	解释
IPv6 ICMP: sent	发送 ICMP 数据报
type <129>	Ping 协议号
src <2003::1>	源 IPv6 地址
dst <2003::20a:ebff:fe26:8a49>	目的 IPv6 地址
from Vlan1	发送的三层端口

1.2.7 debug ipv6 nd

命令：debug ipv6 nd [ns | na | rs | ra | redirect]

no debug ipv6 nd [ns | na | rs | ra | redirect]

功能：打开指定类型的 IPv6 ND 协议报文收发调试开关，其中 ns, na, rs, ra 和 redirect 分别表示邻居请求，邻居公告，路由器请求，路由器公告和路由重定向，如果不指定其中任何一种类型，则表示同时打开所有 5 种类型的 ND 报文收发调试开关。本命令的 no 操作关闭指定类型的 IPv6 ND 协议报文收发调试开关，如果不指定类型，则关闭所有 5 种 ND 报文收发调试开关。

参数：无。

缺省情况：IPv6 ND 的所有 5 种协议报文收发调试开关默认是关闭的。

命令模式：特权模式。

使用指南：ND 协议是 IPv6 的一个核心协议，使用本命令可以显示指定类型的 ND 协议报文，达到诊断排错的目的。

举例：

Switch#debug ipv6 nd

IPv6 ND: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

显示内容	解释
IPv6 ND: rcvd	接收 ND 数据报
type <136>	ND 类型
src <fe80::203:fff:fe01:2786>	源 IPv6 地址
dst <fe80::203:fff:fe01:59ba>	目的 IPv6 地址

1.2.8 debug ipv6 tunnel packet

命令：debug ipv6 tunnel packet

no debug ipv6 tunnel packet

功能：tunnel 数据包收发调试信息。

参数：无。

缺省情况：无。

命令模式：特权模式。

使用指南：

举例：

Switch#debug ipv6 tunnel packet

IPv6 tunnel: rcvd, type <136>, src <fe80::203:fff:fe01:2786>, dst <fe80::203:fff:fe01:59ba>

IPv6 tunnel packet : rcvd src 178.1.1.1 dst 179.2.2.2 size 128 from tunnel1

显示内容	解释
IPv6 tunnel packet : rcvd	接收隧道数据报
type <136>	ND 类型

src 178.1.1.1 dst	隧道源 IPv4 地址
dst 179.2.2.2	隧道目的 IPv4 地址

1.2.9 description

命令：description <desc>

no description

功能：配置隧道的描述信息，本命令的no操作删除隧道描述信息。

参数：<desc>为隧道的描述信息，它是长度不超过256的字符串。

命令模式：隧道配置模式。

缺省情况：隧道缺省没有配置描述信息。

使用指南：在系统中有多条隧道时，配置描述信息有助于用户识别不同隧道的用途。

举例：配置隧道描述为toCernet2。

Switch(Config-if-Tunnel1)#description toCernet2

1.2.10 ipv6 proxy enable

本交换机不支持此命令。

1.2.11 ip address

命令：ip address <ipaddress> <mask> [secondary]

no ip address [<ipaddress> <mask>] [secondary]

功能：设置交换机的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。

参数：<ipaddress>为 IP 地址，点分十进制格式；<mask>为子网掩码，点分十进制格式；[secondary]为表示配置的 IP 地址为从 IP 地址。

命令模式：VLAN 接口配置模式。

缺省情况：系统缺省没有 IP 地址配置。

使用指南：本命令为在 VLAN 接口手工配置 IP 地址，若没有配置可选参数 secondary，表示配置为 VLAN 接口的主 IP 地址，若配置了可选参数 secondary，则表示该 IP 地址为 VLAN 接口的从 IP 地址。一个 VLAN 接口只能有一个主 IP 地址，可以有多个从 IP 地址。主 IP 和从 IP 均可以用于 SNMP/Web/Telnet 管理。此外，交换机还提供了 BOOTP/DHCP 方式获取 IP 地址。

举例：交换机 VLAN1 接口的 IP 地址设置为 192.168.1.10/24。

Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

1.2.12 ipv6 address

命令：ipv6 address <ipv6address/prefix-length> [eui-64]

no ipv6 address <ipv6address/prefix-length> [eui-64]

功能：为接口配置可聚合全球单播地址、本地站点地址、本地链路地址。

参数：*<ipv6address>*参数为 IPv6 地址的前缀，*<prefix-length>*参数为 IPv6 地址的前缀长度，前缀长度为 3-128 之间，**eui-64** 表明根据接口的 eui64 接口标识符自动生成 IPv6 地址。

命令模式：接口配置模式。

缺省情况：无。

使用指南：IPv6 地址前缀不能是多播地址，及其它有特定用途的 IPv6 地址，不同的 vlan 三层接口不能配置相同的地址前缀。对于全球单播地址，前缀长度必须大于或等于 3。对于本地站点地址和本地链路地址，前缀长度必须大于或等于 10。对于 interface loopback 接口，前缀长度必须等于 128。

举例：在 Vlan1 三层接口上配置一个 IPv6 地址：前缀为 2001:3f:ed8::99，前缀长度为 64。

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

1.2.13 ipv6 route

命令：`ipv6 route <ipv6-prefix/prefix-length> {<ipv6address> |<interface-type interface-number>|{<ipv6address> <interface-type interface-number>}} | tunnel <tunnel no> } [<precedence>]`
`no ipv6 route <ipv6-prefix/prefix-length> {<ipv6address> |<interface-type interface-number>|{<ipv6address> <interface-type interface-number>}} | tunnel <tunnel no> } [<precedence>]`

功能：设置 IPv6 静态路由。

参数：*<ipv6-prefix>*参数为 IPv6 网络静态路由的目的地址，*<prefix-length>*参数为 IPv6 前缀长度，*<ipv6address>*参数为可以到达指定网络的下一跳 IPv6 地址，*<interface-type interface-number>*参数为指向静态路由出口接口名，*<tunnel no>* 参数为隧道路由的出口隧道号，*<precedence>*参数为本路由的权重，范围为 1-255,默认为 1。

缺省情况：没有配置任何的 IPv6 静态路由。

命令模式：全局配置模式。

使用指南：在下一跳 IPv6 地址为本地链路地址时，必须指定出口的接口名。下一跳 IPv6 地址为全球可聚合单播地址和本地站点地址时，当不指定出口的接口名，必须保证该下一跳的 IP 地址和交换机某一接口的地址在同一个网段内。对于隧道路由可以直接指定接口名。

举例：配置静态路由 1，目的地址为 3ffe:589:dfc::88，前缀长度为 64，下一跳为 2001:8fd:c32::99（该路由器已经配置了 2001:8fd:c32::34/64 的 IPv6 地址）。

```
Switch(config)#ipv6 route 3ffe:589:dfc::88/64 2001:8fd:c32::99
```

配置静态路由 2，目的地址为 3ffe:ff7:123::55，前缀长度为 64，下一跳为 fe80::203:ff:89fd:46ac,出接口名为 Vlan1。

```
Switch(config)#ipv6 route 3ffe:ff7:123::55/64 fe80::203:ff:89fd:46ac Vlan1
```

1.2.14 ipv6 redirect

命令：`ipv6 redirect`

`no ipv6 redirect`

功能：使能 IPv6 路由重定向功能，本命令的 no 操作为关闭 IPv6 路由重定向功能。

参数：无。

命令模式：全局配置模式。

缺省情况：IPv6 路由重定向功能缺省是关闭的。

使用指南：如果路由器 A、路由器 B 和节点 C 位于同一网络链路，路由器 A 把来自节点 C 的 IPv6 数据包转发到路由器 B，希望路由器 B 继续转发该数据包，则路由器 A 会向数据包源节点 C 发送 IPv6 ICMPv6 路由重定向报文，告知数据包源点 C 发往该目的地址的最优下一跳是路由器 B，这样节省了路由器 A 的转发开销，也缩短了节点 C 的网络传输延迟。

举例：打开 IPv6 路由重定向功能。

```
Switch(config)# ipv6 redirect
```

1.2.15 ipv6 nd dad attempts

命令：ipv6 nd dad attempts <value>

no ipv6 nd dad attempts

功能：设置重复地址检测时接口连续发出的邻居请求消息数目。

参数：<value>参数为重复地址检测连续发出的邻居请求消息数目，<value>值必须在 0-10 之间，no 命令为恢复到默认值 1。

命令模式：接口配置模式。

缺省情况：缺省的请求消息数目为 1

使用指南：当在接口上配置一个 IPv6 地址时，要执行 IPv6 重复地址检测，该命令用于配置需要发送的重复地址检测的 ND 报文数量，value 为 0 则不进行重复地址检测。

举例：设置重复地址检测时接口连续发出的邻居请求消息数目为 3。

```
Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3
```

1.2.16 ipv6 nd ns-interval

命令：ipv6 nd ns-interval <seconds>

no ipv6 nd ns-interval

功能：设置接口发送邻居请求消息的时间间隔。

参数：<seconds>参数为发送邻居请求消息的时间间隔，<seconds>值必须在 1-3600 秒之间，no 命令为恢复到默认值 1 秒。

命令模式：接口配置模式。

缺省情况：缺省的请求消息时间间隔为 1 秒。

使用指南：该设定的值将包含在该接口上所有的路由公告消息中，在一般的情况下不推荐非常短的时间间隔。

举例：设置 Vlan1 接口发送邻居请求消息的时间间隔为 8 秒。

```
Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8
```

1.2.17 ipv6 nd suppress-ra

命令：ipv6 nd suppress-ra

no ipv6 nd suppress-ra

功能：禁止路由器公告。

参数：无。

命令模式：接口配置模式。

缺省情况：没有启动路由公告功能。

使用指南：no ipv6 nd suppress-ra 命令开启路由公告功能。

举例：打开路由公告功能。

Switch(Config-if-Vlan1)#no ipv6 nd suppress-ra

1.2.18 ipv6 nd ra-lifetime

命令：ipv6 nd ra-lifetime <seconds>

no ipv6 nd ra-lifetime

功能：配置路由器公告的生存期。

参数：<seconds>参数表示路由器公告生存期的秒数，<seconds>值必须为 0-9000 之间。

命令模式：接口配置模式。

缺省情况：路由器缺省公告生存期的秒数为 1800。

使用指南：该命令用于配置三层接口上路由器的生存时间，seconds 为 0 说明此接口不能用于默认路由器，否则该值不应该小于发送路由公告的最大时间间隔。如果不进行配置，该值等于发送路由公告的最大时间间隔的 3 倍。

举例：设置路由公告的生存期为 100 秒。

Switch (Config-if-Vlan1)#ipv6 nd ra-lifetime 100

1.2.19 ipv6 nd min-ra-interval

命令：ipv6 nd min-ra-interval <seconds>

no ipv6 nd min-ra-interval

功能：设置发送路由公告的最小时间间隔。

参数：<seconds>参数为发送路由公告的最小时间间隔秒数，<seconds>值必须为 3-1350 秒之间。

命令模式：接口配置模式。

缺省情况：发送路由公告缺省的最小时间间隔为 200 秒。

使用指南：路由公告的最小时间间隔不超过最大时间间隔的 3/4。

举例：设置发送路由公告的最小时间间隔为 10 秒。

Switch (Config-if-Vlan1)#ipv6 nd min-ra-interval 10

1.2.20 ipv6 nd max-ra-interval

命令：ipv6 nd max-ra-interval <seconds>

no ipv6 nd max-ra-interval

功能：设置发送路由公告的最大时间间隔。

参数：<seconds>参数为发送路由公告的时间间隔秒数，<seconds>值必须为 4-1800 秒之间。

命令模式：接口配置模式。

缺省情况：发送路由公告缺省的最大时间间隔为 600 秒。

使用指南：路由公告的最大时间间隔要小于路由公告的生存期的值。

举例：设置发送路由公告的最大时间间隔为 20 秒。

Switch (Config-if-Vlan1)#ipv6 nd max-ra-interval 20

1.2.21 ipv6 nd prefix

命令： `ipv6 nd prefix <ipv6-prefix/prefix-length> { [<valid-lifetime> <preferred-lifetime>] [ no-autoconfig | off-link [no-autoconfig] ] }`

no ipv6 nd prefix <ipv6-prefix/prefix-length>

功能：配置用于路由器公告的地址前缀以及相关参数。

参数： **<ipv6-prefix>**参数为指定要公告的地址前缀，**<prefix-length>**参数为指定要公告的地址前缀的长度，**<valid-lifetime>**参数为该前缀的有效生存期，**<preferred-lifetime>**参数为该前缀的优先生存期，有效生存期必须不小于优先生存期。**no-autoconfig** 参数说明在本地链路的主机上不能使用该前缀来自动配置 IPv6 地址，**off-link** 参数说明路由器公告消息指定的前缀不分配给本地链路，向包含这个指定前缀的地址发送数据的节点认为目的地是本地链路不可达的。

命令模式：接口配置模式。

缺省情况：**valid-lifetime** 的默认值是 2592000 秒(30 天)，**preferred-lifetime** 的默认值是 604800 秒(7 天)。**off-link** 默认是关闭的，**no-autoconfig** 默认是关闭的。

使用指南：该命令允许控制每一个 IPv6 前缀的路由器公告参数，注意有效生存期和优先生存期必须同时配置。

举例：在 Vlan1 配置 IPv6 公告前缀为 2001:410:0:1::/64，该前缀有效生存期为 8640 秒，优先生存期为 4320 秒。

Switch (Config-if-Vlan1)#ipv6 nd prefix 2001:410:0:1::/64 8640 4320

1.2.22 ipv6 nd ra-hoplimit

命令： `ipv6 nd ra-hoplimit <value>`

功能：设置发送路由公告的 hoplimit 值。

参数：**<value>**参数为发送路由公告的 hoplimit 值，**<value>**值必须为 0-255 之间。

命令模式：接口配置模式。

缺省情况：发送路由公告缺省的 hoplimit 值为 64。

举例：设置 interface vlan 1 内发送的路由公告的 hoplimit 值为 128。

Switch#(config-if-vlan1)#ipv6 nd ra-hoplimit 128

1.2.23 ipv6 nd ra-mtu

命令： `ipv6 nd ra-mtu <value>`

功能：设置发送路由公告的 mtu 值。

参数：**<value>**参数为发送路由公告的 mtu 值，**<value>**值必须为 0-1500 之间。

命令模式：接口配置模式。

缺省情况：发送路由公告缺省的 mtu 值为 1500。

举例：设置 interface vlan 1 内发送的路由公告的 mtu 值为 500。

Switch(config-if-vlan1)#ipv6 nd ra-mtu 500

1.2.24 ipv6 nd reachable-time

命令：ipv6 nd reachable-time <seconds>

功能：设置发送路由公告的 reachable-time 值。

参数：<seconds> 参数为发送路由公告的 reachable-time 值，<seconds> 值必须为 0-3600000 毫秒之间。

命令模式：接口配置模式。

缺省情况：发送路由公告缺省的 reachable-time 值为 30000 毫秒。

举例：设置 interface vlan 1 内发送的路由公告的 reachable-time 值为 100000 毫秒。

Switch(config-if-vlan1)#ipv6 nd reachable-time 100000

1.2.25 ipv6 nd retrans-timer

命令：ipv6 nd retrans-timer <seconds>

功能：设置发送路由公告的 retrans-timer 值。

参数：<seconds> 参数为发送路由公告的 retrans-timer 值，<seconds> 值必须为 0-4294967295 毫秒之间。

命令模式：接口配置模式。

缺省情况：发送路由公告缺省的 retrans-timer 值为 1000 毫秒。

举例：设置 interface vlan 1 内发送的路由公告的 retrans-timer 值为 10000 毫秒。

Switch(config-if-vlan1)#ipv6 nd retrans-timer 10000

1.2.26 ipv6 nd other-config-flag

命令：ipv6 nd other-config-flag

功能：设置发送路由公告的其他状态配置标志为 1。

参数：无。

命令模式：接口配置模式。

缺省情况：路由公告的其他状态配置标志默认为 0。

使用指南：当其他状态配置标志为 1 时，表示收到这个路由公告的主机必须使用有状态地址配置协议(比如 DHCPv6)来获得非地址配置的信息(比如 DNS 地址等)。

举例：设置发送路由公告的其他状态配置标志。

Switch(config-if-vlan1)#ipv6 nd other-config-flag

1.2.27 ipv6 nd managed-config-flag

命令：ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

功能：设置发送路由公告的管理地址配置标志为 1。

参数：无。

命令模式：接口配置模式。

缺省情况：路由公告的管理地址配置标志默认为 0。

使用指南：当管理地址配置标志为 1 时，表示收到这个路由公告的主机除了可能按照无状态地址自动配置协议获得地址外，还必须使用有状态地址配置协议(比如 DHCPv6)来获得地址；当管理地址配置标志为 0 时，表示收到这个路由公告的主机只使用无状态地址自动配置协议获得地址。

举例：设置发送路由公告的管理地址配置标志。

Switch(config-if-vlan1)#ipv6 nd managed-config-flag

1.2.28 ipv6 neighbor

命令：ipv6 neighbor <ipv6address> <hardware-address> interface <interface-type interface-name>

no ipv6 neighbor <ipv6address>

功能：设置静态邻居表项。

参数：ipv6address 参数为静态邻居 IPv6 地址，与接口前缀相同，hardware-address 参数为静态邻居硬件地址，interface-type 为 ethernet 类型，interface-name 为二层接口名。

命令模式：接口配置模式。

缺省情况：没有静态邻居表项。

使用指南：不能将用于特殊用途的 IPv6 地址和多播地址，及本机地址设置为邻居。

举例：在端口 E1/1 上设置静态邻居 2001:1:2::4，硬件 MAC 地址为 00-03-0f-89-44-bc。

Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet 1/1

1.2.29 interface tunnel

命令：interface tunnel <tnl-id>

no interface tunnel <tnl-id>

功能：创建/删除隧道。

参数：<tnl-id> 参数为隧道号。

命令模式：全局配置模式。

缺省情况：无。

使用指南：该命令创建一个虚拟的隧道接口，由于没有指定隧道的模式和隧道源等信息，show ipv6 tunnel 没有显示该隧道，创建后进入隧道模式，在该模式下可以指定隧道的源、目的等信息。no 命令是删除一条隧道。

举例：创建隧道 1。

Switch(Config)#interface tunnel 1

1.2.30 show ip interface

命令：show ip interface [<ifname> | vlan <vlan-id>] brief

功能：显示配置的三层接口的简要信息。

参数：<ifname>为接口名称；<vlan-id>为 VLAN 号。

缺省情况：不指定参数时，显示所有配置的三层接口的简要信息。

命令模式：所有模式

使用指南：无。

举例：Restarter#show ip interface vlan1 brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	192.168.2.11	up

1.2.31 show ip traffic

命令：show ip traffic

功能：显示 IP 数据包统计信息。

命令模式：特权用户配置模式。

使用指南：显示 IP，ICMP，TCP，UDP 数据包的接收、发送等统计信息。

举例：

Switch #show ip traffic

IP statistics:

Rcvd: 3249810 total, 3180 local destination

0 header errors, 0 address errors

0 unknown protocol, 0 discards

Frgs: 0 reassembled, 0 timeouts

0 fragment rcvd, 0 fragment dropped

0 fragmented, 0 couldn't fragment, 0 fragment sent

Sent: 0 generated, 3230439 forwarded

0 dropped, 0 no route

ICMP statistics:

Rcvd: 0 total 0 errors 0 time exceeded

0 redirects, 0 unreachable, 0 echo, 0 echo replies

0 mask requests, 0 mask replies, 0 quench

0 parameter, 0 timestamp, 0 timestamp replies

Sent: 0 total 0 errors 0 time exceeded

0 redirects, 0 unreachable, 0 echo, 0 echo replies

0 mask requests, 0 mask replies, 0 quench

0 parameter, 0 timestamp, 0 timestamp replies

TCP statistics:

TcpActiveOpens 0, TcpAttemptFails 0

TcpCurrEstab 0, TcpEstabResets 0

TcpInErrs 0, TcpInSegs 3180

TcpMaxConn 0, TcpOutRsts 3

TcpOutSegs	3, TcpPassiveOpens	8
TcpRetransSegs	0, TcpRtoAlgorithm	0
TcpRtoMax	0, TcpRtoMin	0
UDP statics:		
UdpInDatagrams	0, UdpInErrors	0
UdpNoPorts	0, UdpOutDatagrams	0

显示信息	解释
IP statistics:	IP 数据包的统计信息:
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	接收总量的统计及其中有多少到达本地、多少数据包的包头有错误、多少地址有错误、多少不明协议的数据包、多少丢包等的统计。
Frgs: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	分段统计: 重组多少数据包、超时的有多少、接收分段数、丢失分段数、多少不能分段、发送多少分段等。
Sent: 0 generated, 3230439 forwarded 0 dropped, 0 no route	发送总量的统计及其中包括多少从本地产生的、多少是转发的、多少丢失的、多少没有路由的等。
ICMP statistics:	ICMP 数据包的统计信息:
Rcvd: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	接收 ICMP 数据包总量的统计及将这些 ICMP 数据包进行分类, 分类后的统计数据。
Sent: 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	发送 ICMP 数据包总量的统计及将这些 ICMP 数据包进行分类, 分类后的统计数据。
TCP statistics:	TCP 数据包统计信息:
TcpActiveOpens 0, TcpAttemptFails 0 TcpCurrEstab 0, TcpEstabResets 0 TcpInErrs 0, TcpInSegs 3180 TcpMaxConn 0, TcpOutRsts 3 TcpOutSegs 3, TcpPassiveOpens 8 TcpRetransSegs 0, TcpRtoAlgorithm 0 TcpRtoMax 0, TcpRtoMin 0	主动打开连接数, 失败重试次数。 当前建立连接数, 连接重置数 接收错误数据包, 接收的段内数据包数 最大连接数, 输出重置数 输出分段数据包数, 被动连接数 重传数据包数, 重传定时器时间 重传定时器允许最大时间, 重传定时器允许最小时间
UDP statics:	UDP 数据包统计信息:
UdpInDatagrams 0, UdpInErrors 0 UdpNoPorts 0, UdpOutDatagrams 0	接收的 UDP 数据包, 接收的错误数据包。 无端口数据包数, 发送数据包数

1.2.32 show ipv6 interface

命令：show ipv6 interface {brief}[interface-name]}

功能：显示接口 IPv6 参数。

参数：brief 参数为 IPv6 状态和配置简要概括, interface-name 参数为三层接口名。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：如果只是指定 brief，则显示所有三层接口的信息，也可以指定具体某一个三层接口。

举例：

```
Switch#show ipv6 interface Vlan1
Vlan1 is up, line protocol is up, dev index is 2004
Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)
IPv6 is enabled
Link-local address(es):
  fe80::203:fff:fe00:10 PERMANENT
Global unicast address(es):
  3001::1 subnet is 3001::1/64 PERMANENT
Joined group address(es):
  ff02::1
  ff02::16
  ff02::2
  ff02::5
  ff02::6
  ff02::9
  ff02::d
  ff02::1:ff00:10
  ff02::1:ff00:1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
ND RA MTU is 0
ND advertised reachable time is 0 millisecond(s)
ND advertised retransmit time is 0 millisecond(s)
```

显示内容	解释
Vlan1	三层接口名
[up/up]	三层接口状态
dev index	内部索引号
fe80::203:fff:fe00:10	三层接口自动配置的 IPv6 地址
3001::1	三层接口配置的 IPv6 地址

1.2.33 show ipv6 route

命令：show ipv6 route [<destination> | <destination > | <length> | database | fib [local] | nsm [connected | static | rip | ospf | bgp | isis | kernel | database] | statistics]

功能：显示 IPv6 路由表。

参数：<destination> 为目标网络地址；<destination >/<length> 为目标网络地址加上前缀长度；connected 为直连路由；static 为静态路由；rip 为 RIP 路由；ospf 为 OSPF 路由；bgp 为 BGP 路由；isis 为 ISIS 路由；kernel 为核心路由；statistics 显示路由条数；database 为路由数据库。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：show ipv6 route 只显示 IPv6 核心路由表(tcpip 中的路由表)，database 显示除本地路由中的所有路由，fib local 显示本地路由，statistics 显示路由统计信息。

举例：

Switch#show ipv6 route

Codes: C - connected, L - Local, S - static, R - RIP, O - OSPF,
I - IS-IS, B - BGP

```

C   ::/0   via ::,   tunnel3   256
S   2001:2::/32   via fe80::789,   Vlan2   1024
S   2001:2:3:4::/64   via fe80::123,   Vlan2   1024
O   2002:ca60:c801:1::/64   via ::,   Vlan1   1024
C   2002:ca60:c802:1::/64   via ::,   tunnel49   256
C   2003:1::/64   via ::,   Vlan4   256
C   2003:1::5efe:0:0/96   via ::,   tunnel26   256
S   2004:1:2:3::/64   via fe80:1::88,   Vlan2   1024
O   2006:1::/64   via ::,   Vlan1   1024
S   2008:1:2:3::/64   via fe80::250:baff:fef2:a4f4,   Vlan1   1024
C   2008:2005:5:8::/64   via ::,   Ethernet0   256
S   2009:1::/64   via fe80::250:baff:fef2:a4f4,   Vlan1   1024
C   2022:1::/64   via ::,   Ethernet0   256
O   3333:1:2:3::/64   via fe80::20c:ceff:fe13:eac1,   Vlan12   1024
C   3ffe:501:ffff:1::/64   via ::,   Vlan4   256
O   3ffe:501:ffff:100::/64   via ::,   Vlan5   1024
O   3ffe:3240:800d:1::/64   via ::,   Vlan1   1024
O   3ffe:3240:800d:2::/64   via ::,   Vlan2   1024

```

- O 3ffe:3240:800d:10::/64 via ::, Vlan12 1024
- O 3ffe:3240:800d:20::/64 via fe80::20c:ceff:fe13:eac1, Vlan12 1024
- C fe80::/64 via ::, Vlan1 256
- C fe80::5efe:0:0/96 via ::, tunnel26 256
- C ff00::/8 via ::, Vlan1 256

显示内容	解释
IPv6 Routing Table	IPv6 路由表情况
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP, * - selected route, * - FIB route, p - stale info	各个项的缩写显示标记
S 2009:1::/64 via fe80::250:baff:fef2:a4f4, Vlan1 1024	FIB 表中的静态路由，目的网段为 2002::/64，via 表示通过 fe80::250:baff:fef2:a4f4 为下一跳，Vlan1 为出接口名，1024 为路由权重

1.2.34 show ipv6 neighbors

命令： show ipv6 neighbors [{vlan|ethernet|tunnel } interface-number | interface-name | address <ipv6address>]

功能：显示邻居表项信息。

参数：{vlan|ethernet|tunnel } *interface-number* 和 *interface-name* 参数指定按接口名或者端口名进行查找。**address <ipv6address>**参数指定按 IPv6 地址进行查找。当没有指定参数时，本命令显示所有的邻居表项。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：

举例：

Switch#show ipv6 neighbors

IPv6 neighbour unicast items: 14, valid: 11, matched: 11, incomplete: 0, delayed: 0,
manage items 5

IPv6 Address	Hardware Addr	Interface	Port
2002:ca60:c801:1:250:baff:fef2:a4f4	00-50-ba-f2-a4-f4		Vlan1
Ethernet1/2 reachable			
3ffe:3240:800d:1::100	00-03-0f-01-27-86		Vlan1
Ethernet1/3 reachable			
3ffe:3240:800d:1::8888	00-02-01-00-00-00		Vlan1
Ethernet1/1 permanent			
3ffe:3240:800d:1:250:baff:fef2:a4f4	00-50-ba-f2-a4-f4		Vlan1
Ethernet1/4 reachable			
3ffe:3240:800d:2::8888	00-02-01-00-01-01		Vlan2

```

Ethernet1/16    permanent
3ffe:3240:800d:2:203:fff:fe01:2786      00-03-0f-fe-30-45      Vlan2
Ethernet1/15    reachable
fe80::203:fff:fe01:2786                  00-03-0f-01-27-86      Vlan1
Ethernet1/5     reachable
fe80::203:fff:fe01:2786                  00-03-0f-fe-30-45      Vlan2
Ethernet1/17    reachable
fe80::20c:ceff:fe13:eac1                 00-0c-ce-13-ea-c1      Vlan12
Ethernet1/20    reachable
fe80::250:baff:fe02:a4f4                 00-50-ba-f2-a4-f4      Vlan1
Ethernet1/6     reachable

```

IPv6 neighbour table: 11 entries

显示内容	解释
IPv6 Address	邻居 IPv6 地址
Hardware Addr	邻居 MAC 地址
Interface	出接口名
Port	出端口名
State	邻居状态(reachable、stale、delay、probe、permanent、incomplete、unknown)

1.2.35 show ipv6 traffic

命令：show ipv6 traffic

功能：显示 IPv6 转发数据包统计信息。

参数：无。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：

举例：

Switch#show ipv6 traffic

IP statistics:

Rcvd: 90 total, 17 local destination

0 header errors, 0 address errors

0 unknown protocol, 13 discards

Frgs: 0 reassembled, 0 timeouts

0 fragment rcvd, 0 fragment dropped

0 fragmented, 0 couldn't fragment, 0 fragment sent

Sent: 110 generated, 0 forwarded

0 dropped, 0 no route

ICMP statistics:

Rcvd: 0 total 0 errors 0 time exceeded

0 redirects, 0 unreachable, 0 echo, 0 echo replies

显示内容	解释
IP statistics	IPv6 数据报统计
Rcvd: 90 total, 17 local destination0 header errors, 0 address errors0 unknown protocol, 13 discards	IPv6 收包统计
Frgs: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 分片统计
Sent: 110 generated, 0 forwarded 0 dropped, 0 no route	IPv6 发包统计

1.2.36 show ipv6 redirect

命令：show ipv6 redirect

功能：显示 IPv6 重定向开关状态。

参数：无。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：本命令可用于了解系统中 IPv6 路由重定向功能是否启用。

举例：

```
Switch#show ipv6 redirect
ipv6 redirect is disabled
```

1.2.37 show ipv6 tunnel

命令：show ipv6 tunnel [<tnl-id>]

功能：显示隧道信息。

参数：<tnl-id> 参数为隧道号。

缺省情况：无。

命令模式：特权和配置模式。

使用指南：如果不加隧道号，显示所有隧道的信息，如果带有隧道号将显示指定隧道的详细信息。

举例：

```
Switch#show ipv6 tunnel
name      mode      source      destination      nexthop
tunnel3   6to4      178.1.1.1
```

显示内容	解释
Name	隧道名
mode	隧道类型
source	隧道源 ipv4 地址
destination	隧道目的 ipv4 地址
nexthop	隧道下一跳（只适用于 ISATAP 隧道）

1.2.38 tunnel source

命令：tunnel source {<ipaddress> | <ipv6address> | <interface-name>}
no tunnel source

功能：配置隧道源点的IPv4/IPv6地址。

参数：<ipaddress> 为隧道源点的IPv4地址，<ipaddress> 必须是单播地址；
<ipv6address>为隧道源点的IPv6地址；<interface-name> 表示隧道源地址取自接口
<interface-name>的主IPv4地址。

命令模式：隧道配置模式。

缺省情况：隧道缺省没有配置源点的IPv4/IPv6地址，也没有配置隧道源接口名。

使用指南：配置任何类型的隧道都必须配置源点的IPv4/IPv6地址或指定一个借用隧道源地
址的接口名。

举例：配置隧道源点IPv4地址为202.89.176.6。

Switch(Config-if-Tunnel1)#tunnel source 202.89.176.6

1.2.39 tunnel destination

命令：tunnel destination <ipaddress | ipv6address>
no tunnel destination

功能：配置隧道终点的IPv4/IPv6地址。

参数：<ipaddress> 为隧道终点的IPv4地址，<ipv6address> 为隧道终点的IPv6地址。

命令模式：隧道配置模式。

缺省情况：隧道缺省没有配置终点的IPv4/IPv6地址。

使用指南：该命令仅适用于手工隧道，用于配置手工隧道的终点IPv4/IPv6地址。

举例：配置隧道终点IPv4地址为203.78.120.5。

Switch(Config-if-Tunnel1)#tunnel destination 203.78.120.5

1.2.40 tunnel nexthop

命令：tunnel nexthop <ipaddress>
no tunnel nexthop

功能：配置隧道下一跳的IPv4地址。

参数：<ipaddress> 为隧道下一跳的IPv4地址。

命令模式：隧道配置模式。

缺省情况： 隧道缺省没有配置下一跳IPv4地址。

使用指南： 该命令仅适用于ISATAP隧道，其它类型的隧道不会检查nexthop的配置。注意，ISATAP隧道的下一跳IPv4地址必须和隧道源的IPv4地址在同一网段。

举例： 配置ISATAP隧道的下一跳ipv4地址为178.99.156.8。

```
Switch(Config-if-Tunnel1)#tunnel source 178.99.156.7
```

```
Switch(Config-if-Tunnel1)#tunnel nexthop 178.99.156.8
```

```
Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap
```

1.2.41 tunnel 6to4-relay

本型号交换机不支持此命令。

1.2.42 tunnel mode

命令： **tunnel mode** **[[gre] | ipv6ip [6to4 | isatap]]**
no tunnel mode

功能： 配置隧道模式。

参数： gre 为 GRE 隧道。

命令模式： 隧道配置模式。

缺省情况： 无。

使用指南： 在配置隧道模式的时候，只指定 ipv6ip 表明是配置隧道。ipv6ip 6to4 表明是 6to4 隧道，ipv6ip isatap 表明是 ISATAP 隧道。

举例： 配置隧道模式

1、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip

2、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip 6to4

3、Switch(Config-if-Tunnel1)#tunnel mode ipv6ip isatap

1.3 网管端口配置命令

1.3.1 duplex

本交换机不支持此命令。

1.3.2 interface ethernet

命令： **interface ethernet** **<interface-name>**

功能： 从全局配置模式进入到网管端口配置模式。

参数： **<interface-name>**为端口号，取 0 或 1。

命令模式： 全局配置模式。

使用指南： 使用命令 **exit** 可从以网管端口配置模式退回到全局配置模式。interface ethernet 1 为 CP 上的网管口，interface ethernet 0 为 SAIC 卡上的网管口。

举例：进入网管端口。

```
Switch(config)#interface ethernet 0
```

```
Switch(Config-If-Ethernet0)#
```

1.3.3 ip address

命令：ip address <ip-address> <mask>

no ip address [<ip-address> <mask>]

功能：设置交换机的 IP 地址及掩码；本命令的 no 操作为删除该 IP 地址配置。

参数：<ip-address>为 IP 地址，点分十进制格式；<mask>为子网掩码，点分十进制格式。

命令模式：网管端口配置模式。

缺省情况：系统缺省没有 IP 地址配置。

使用指南：本命令为在网管端口配置 IP 地址。

举例：网管端口的 IP 地址设置为 192.168.1.10/24。

```
Switch(Config-If-Ethernet0)#ip address 192.168.1.10 255.255.255.0
```

1.3.4 shutdown

命令：shutdown

no shutdown

功能：关闭网管端口；本命令的 no 操作为打开端口。

命令模式：网管端口配置模式。

缺省情况：网管端口缺省为打开。

使用指南：当关闭网管端口时，网管端口将不发送数据帧，并且在用户输入 **show interface** 命令时显示端口状态为 down。

举例：打开网管端口。

```
Switch(config)#interface ethernet 0
```

```
Switch(Config-If-Ethernet0)#no shutdown
```

1.3.5 speed

本交换机不支持此命令。

1.4 IP路由聚合配置命令

1.4.1 ip fib optimize

命令：ip fib optimize

no ip fib optimize

功能：配置交换机使用优化 IP 路由聚合算法；本命令的 no 操作为交换机不使用优化 IP 路由聚合算法。

缺省情况：出厂时不使用优化 IP 路由聚合算法。

命令模式：全局配置模式。

使用指南：该命令是为了实现对聚合算法的优化，优化方法为：如果路由表不具备缺省路由，根据被引用最多的下一跳构造一个虚拟缺省路由，以简化聚合的结果。使用该方式的好处是更有效的简化了聚合的结果；缺点是虽然降低了（通过将虚拟缺省路由加入芯片网段路由表项）本交换机 CPU 负载，但是可能会为下一跳交换机引入不必要的数据流（实际上为将部分本交换机 CPU 负载转给了下一跳交换机）。

举例：配置交换机不使用优化 IP 路由聚合算法。

Switch(config)#no ip fib optimize

1.5 URPF命令

1.5.1 debug urpf

命令：debug urpf {notice | warn | error}

no debug urpf {notice | warn | error}

功能：打开 URPF 调试功能，在 URPF 规则安装失败时提示错误。

命令模式：特权模式。

参数：无。

使用指南：无。

举例：

Switch#debug urpf error

1.5.2 ip urpf enable

命令：ip urpf enable {loose | strict} {allow-default-route }

no ip urpf enable

功能：使能端口上的 URPF 功能。

参数： loose：松散类型；

strict：严格类型；

allow-default-route：允许缺省路由。

命令模式：端口配置模式。

缺省情况：端口不打开 URPF 功能。

使用指南：要指明是严格或者松散模式。

举例：

Switch(config)#interface ethernet 1/4

Switch(Config-If-Ethernet1/4)#ip urpf enable strict

Switch(Config-If-Ethernet1/4)#interface ethernet 1/5

```
Switch(Config-If-Ethernet1/5)#ip urpf enable loose
Switch(Config-If-Ethernet1/5) #interface ethernet 1/6
Switch(Config-If-Ethernet1/6)#ip urpf enable loose allow-default-route
Switch(Config-If-Ethernet1/6)#interface ethernet 1/7
Switch(Config-If-Ethernet1/7)#ip urpf enable strict allow-default-route
```

1.5.3 show urpf rule ipv4 num

命令：show urpf rule ipv4 num interface {ethernet IFNAME |IFNAME}

功能：显示端口绑定的 ipv4 规则数目。

命令模式：特权和配置模式。

参数：IFNAME：指明端口名字。

使用指南：无。

举例：显示端口 Ethernet1/4 绑定的 IPv4 规则数目。

```
Switch# show urpf rule ipv4 num interface ethernet 1/4
```

1.5.4 show urpf rule ipv6 num

命令：show urpf rule ipv6 num interface {ethernet IFNAME |IFNAME}

功能：显示端口绑定的 ipv6 规则数目。

命令模式：特权和配置模式。

参数：IFNAME：指明端口名字。

使用指南：无。

举例：显示端口 Ethernet1/4 绑定的 IPv6 规则数目。

```
Switch# show urpf rule ipv6 num interface ethernet 1/4
```

1.5.5 show urpf rule ipv4

命令：show urpf rule ipv4 interface {ethernet IFNAME |IFNAME}

功能：显示端口绑定的 ipv4 规则明细。

命令模式：特权和配置模式。

参数：IFNAME：指明端口名字。

使用指南：显示的是当前已经下发的规则。

举例：显示端口 Ethernet1/4 绑定的 IPv4 规则明细。

```
Switch# show urpf rule ipv4 interface ethernet 1/4
```

1.5.6 show urpf rule ipv6

命令：show urpf rule ipv6 interface {ethernet IFNAME |IFNAME}

功能：显示端口绑定的 ipv6 规则明细。

命令模式：特权和配置模式。

参数：IFNAME：指明端口名字

使用指南：显示的是当前已经下发的规则。

举例：显示端口 Ethernet1/4 绑定的 IPv6 规则明细。

Switch# show urpf rule ipv6 interface ethernet 1/4

1.5.7 show urpf

命令：show urpf

功能：显示哪些端口启动了 URPF。

命令模式：特权和配置模式。

参数：无。

使用指南：无。

举例：

Switch#show urpf

1.5.8 urpf enable

命令：urpf enable

no urpf enable

功能：启动全局 URPF 功能。

参数：无。

命令模式：全局配置模式。

缺省情况：系统不启动 URPF 协议模块。

使用指南：无。

举例：

Switch(config)#urpf enable

1.6 ARP转发配置命令

1.6.1 arp

命令：arp <ip_address> <mac_address> {interface [ethernet] <portName>}

no arp <ip_address>

功能：配置静态 ARP 表项；本命令的 no 操作为删除指定 IP 地址的 ARP 表项。

参数：<ip_address>为 IP 地址，与接口在同一字段；<mac_address>为 MAC 地址；**ethernet** 为以太网端口；<portName>为二层端口名称。

缺省情况：缺省没有静态 ARP 表项。

命令模式：VLAN 接口配置模式。

使用指南：在交换机上可以配置静态 ARP 表项。

举例：在接口 vlan 1 配置静态 ARP。

Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/2

1.6.2 clear arp-cache

命令：clear arp-cache

功能：清除交换机学习到的动态 ARP。

命令模式：特权用户配置模式。

举例：

Switch#clear arp-cache

1.6.3 clear arp traffic

命令：clear arp traffic

功能：清除交换机 ARP 报文统计信息。对于机箱交换机，本命令只清除当前板卡的 ARP 报文统计信息。

命令模式：特权用户配置模式

举例：

Switch#clear arp traffic

1.6.4 debug arp

命令：debug arp {receive|send|state}

no debug arp {receive|send|state}

功能：打开 ARP 调试开关；本命令的 no 操作为关闭该调试功能。

参数：receive 交换机接收 ARP 数据包调试开关；send 交换机发送 ARP 数据包调试开关；state 交换机 ARP 状态变化调试开关。

缺省情况：缺省 ARP 调试功能是关闭的。

命令模式：特权用户配置模式。

使用指南：显示接收或发送的 ARP 数据包的内容，包括：类型、源地址、目的地址。

举例：打开 ARP RECEIVE 调试开关。

Switch#debug arp receive

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251, 00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.

%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251,

```
00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.  
e%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251,  
00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.  
%Jan 01 01:05:53 2006 IP ARP: rcvd, type REQUEST, src 172.16.1.251,  
00-e0-4c-88-ad-bc, dst 172.16.1.110, 00-00-00-00-00-00 flag 0x0, pkt type 1, intf Vlan100.
```

1.6.5 ip proxy-arp

命令：ip proxy-arp

no ip proxy-arp

功能：打开 VLAN 接口代理 ARP 的功能；本命令的 no 操作为关闭代理 ARP 的功能。

缺省情况：缺省代理 ARP 功能是关闭的。

命令模式：VLAN 接口配置模式。

使用指南：当交换机的三层接口收到某 ARP 请求，该请求的 IP 地址与三层接口地址在一个 IP 网段，但却不在同一物理网络中，此时该三层接口若启动了代理 ARP 的功能，三层接口会将自己的 MAC 地址作为 ARP 的回应，然后将收到的实际数据报文进行转发。启动该项功能可以使因为物理网络分离但属于同一 IP 网段的机器忽视物理网络分离的事实，经过具有代理 ARP 接口的转发像处在一个物理网络中。代理 ARP 在回应 ARP 请求之前，需要查找路由表，以确定目的网络是否可达，只有目的网络可达的 ARP 请求，才会回应 ARP 请求。注意：匹配了缺省路由的 ARP 请求不进行代理。

举例：打开 VLAN 接口 1 的代理 ARP 功能。

Switch(Config-if-Vlan1)#ip proxy-ar

1.6.6 l3 hashselect

命令：l3 hashselect [<crc16l|crc16u|crc32l|crc32u|lsb>]

功能：设置 L3 表(硬件 ARP 表)HASH 算法。

参数：<crc16l|crc16u|crc32l|crc32u|lsb>为某种具体的 HASH 算法，缺省参数情况下将 L3 表的 HASH 算法设置为默认的 crc32u 算法，系统默认情况下的 HASH 算法为 crc32u。

命令模式：全局配置模式。

使用指南：HASH 算法是一种快速的查找算法，设置 L3 表的 HASH 算法将会改变 ARP 表项在硬件中的存储位置和顺序，该命令的使用主要是为了解决 ARP 表项在硬件表中的冲突。在使用该命令改变 L3 表的 HASH 算法时，用户需要保存配置并重启系统之后新设置的 HASH 算法才会生效，在系统重启之前系统使用的仍然是原来的 HASH 算法。由于所有的 HASH 算法在特定的情况下都会发生 HASH 冲突，所以针对于特定的网络配置需要选择特定的 HASH 算法。经过反复的实验测试和验证，我们对于上述 5 种 HASH 算法的推荐顺序是：crc32u, crc32l, crc16u, crc16l，一般情况下我们不推荐使用 lsb 算法。

使用该命令改变 L3 表的 HASH 算法时，必须要对网络的 ARP 配置做有效的分析，所以该命令必须在厂商技术人员对网络的 ARP 配置做出分析后，在厂商技术人员的指导下使用。

举例：设置 hash 算法为 crc32u。

Switch(Config-if-Vlan1)#l3 hashselect crc32u

1.6.7 show arp

命令： show arp [*<ipaddress>*][*<vlan-id>*][*<hw-addr>*][type {static|dynamic}][count][vrf word]

功能：显示 ARP 映射表。

参数：*<ipaddress>*为显示指定 IP 地址的表项；*<vlan-id>*为显示指定 VLAN 标识的表项；*<hw-addr>*为显示指定 MAC 地址的表项；**static** 为显示静态 ARP 表项；**dynamic** 为显示动态 ARP 表项；**count** 为显示 ARP 表项数量信息；**word** 为要显示的指定 vrf 的名称。

命令模式：特权和配置模式。

使用指南：显示当前 ARP 映射表的内容，如：IP 地址，硬件地址，硬件类型，接口名等。

举例：

Switch#show arp

ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet1/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet1/4	Dynamic

显示信息	解释
Total arp items	ARP 表项的总数；
Valid	符合过滤规则的属于合法状态的 Arp 表项数量；
Matched	符合过滤规则的 Arp 表项数量；
Verifying	处于重验证 Arp 合法性状态的 Arp 表项数量；
InCompleted	发了 Arp request，但未接收到 Arp reply 的 Arp 表项数量；
Failed	处于失效状态的 Arp 表项数量；
None	处于初始创建状态的 Arp 表项数量；
Address	Arp 表项 IP 地址；
Hardware Address	Arp 表项硬件地址；
Interface	Arp 表项对应的三层接口；
Port	Arp 表项对应的物理（二层）端口；
Flag	Arp 表项是动态还是静态说明。

1.6.8 show arp traffic

命令：show arp traffic

功能：显示交换机 ARP 报文统计信息。对于机箱交换机，本命令只统计当前板卡的 ARP 报文收发信息。

命令模式：特权和配置模式。

使用指南：显示 ARP 报文的接收、发送统计信息。

举例：

Switch#show arp traffic

ARP statistics:

Rcvd: 10 request, 5 response

Sent: 5 request, 10 response

1.7 I3 station movement配置命令

1.7.1 I3-station-move

命令：l3-station-move

no l3-station-move

功能：启动 l3-station-move 功能；本命令的 no 操作为关闭 l3-station-move 功能。

正常情况下当出现 arp/nd 切换端口的时候，根据 arp/nd 报文重新学习 arp/nd 表项的端口信息。如果当 PC 或其他网络节点切换端口的时候，没有发送或者接收 ARP 报文的情况我们认为非安全切换，因此不予重新学习。新的“l3 station movement”的功能是为了满足特殊条件下的 arp/nd 切换端口的功能，实现原理为，当打开本功能时候的，如果出现 MAC 切换端口的时候，认为这是安全的网络节点切换，任何从新端口收到的网络报文（src mac 为发生切换的网络节点）触发 arp/nd 切换，重新学习 arp/nd 到新的端口。

参数：<ip_address>为 IP 地址，与接口在同一字段；<mac_address>为 MAC 地址；**ethernet** 为以太网端口；<portName>为二层端口名称。

缺省情况：缺省不启动本功能。

命令模式：全局配置模式。

使用指南：本功能在打开之后，需要进行设备重启才能正确工作。

举例：

```
Switch(Config)# l3-station-move
```

第2章 防ARP扫描功能命令

2.1 anti-arpscan enable [ip|port]

命令：anti-arpscan enable [ip|port]

no anti-arpscan enable [ip|port]

功能：全局启动防 ARP 扫描功能；no 命令全局关闭防 ARP 扫描功能。

参数：无。

缺省情况：缺省时为同时开启或关闭基于 ip 及端口的防 arp 扫描功能。

命令模式：全局配置模式。

使用指南：通过 telnet 等手段远程管理交换机时，必须在启动防 ARP 扫描功能之前将上联端口设置为超级信任端口，以防止此端口收到较多的 ARP 报文而被关闭。在关闭防 ARP 扫描功能之后此端口的属性会恢复为默认值的非信任端口。

举例：在交换机上启动防 ARP 扫描功能。

Switch(config)#anti-arpscan enable ip

2.2 anti-arpscan port-based threshold

命令：anti-arpscan port-based threshold <threshold-value>

no anti-arpscan port-based threshold

功能：设置基于端口的防 ARP 扫描的接收 ARP 报文的阈值，如果接收的 ARP 报文的速率超过此设定值，则关闭此端口。单位为个/秒。no 命令恢复为默认值，即 10 个/秒。

参数：速率阈值，有效范围为 2-200。

缺省情况：10 个/秒。

命令模式：全局配置模式。

使用指南：基于端口的防 ARP 扫描的阈值应该比基于 IP 的防 ARP 扫描的阈值大，否则基于 IP 的防 ARP 扫描将不起作用。

举例：在交换机上配置基于端口的防 ARP 扫描速率阈值为 10 个/秒。

Switch(config)#anti-arpscan port-based threshold 10

2.3 anti-arpscan ip-based level1|level2 threshold

命令：anti-arpscan ip-based level1|level2 threshold <threshold-value>

no anti-arpscan ip-based level1|level2 threshold

功能：设置基于 IP 的防 ARP 扫描的接收 ARP 报文的一级或二级阈值，一级阈值默认为 4p/s，二级默认为 8p/s。二级阈值必须大于一级阈值。

参数：速率阈值，有效范围为 1-200。

缺省情况：一级阈值默认为 4p/s，二级阈值默认为 8p/s。

命令模式：全局配置模式。

使用指南：基于端口的防 ARP 扫描的阈值应该比基于 IP 的防 ARP 扫描的阈值大，否则基于 IP 的防 ARP 扫描将不起作用。

举例：在交换机上配置基于 IP 的防 ARP 扫描速率阈值为 6 个/秒。

```
Switch(Config)# anti-arpscan ip-based level1 threshold 6
```

2.4 anti-arpscan trust

命令：anti-arpscan trust { port | supertrust-port | iptrust-port }
no anti-arpscan trust {port | supertrust-port | iptrust-port}

功能：配置为信任端口或超级信任端口；no 命令恢复为非信任端口。

参数：无。

缺省情况：缺省全部为非信任端口。

命令模式：端口配置模式。

使用指南：如果某端口配置为信任端口，则防 ARP 扫描功能将不对此端口作处理，即使接收到的 ARP 报文速率超过设定的阈值，也不关闭此端口，但对此端口下的非信任 IP 仍然检测。如果配置为超级信任端口，则既不对端口作处理，也不对此端口下的任何 IP 作处理。如果端口已经被防 ARP 扫描关闭，则配置为信任端口后立即打开此端口。如果配置为 IP 信任端口，则不检测此端口下的 IP，紧对端口做处理；如果端口下已有 IP 被禁，则配置为 IP 信任端口后被禁 IP 立即恢复。

通过 telnet 等手段远程管理交换机时，必须在启动防 ARP 扫描功能之前将上联端口设置为超级信任端口，以防止此端口收到较多的 ARP 报文而被关闭。在关闭防 ARP 扫描功能之后此端口的属性会恢复为默认值的非信任端口。

举例：将交换机的端口 ethernet 4/5 配置为信任端口。

```
Switch(config)#interface ethernet4/5
```

```
Switch(Config-if-ethernet 4/5)#anti-arpscan trust port
```

2.5 anti-arpscan trust ip

命令：anti-arpscan trust ip <ip-address> [<netmask>]
no anti-arpscan trust ip <ip-address> [<netmask>]

功能：配置信任 IP；no 命令恢复为非信任 IP。

参数：<ip-address>：要配置的信任 IP 地址；<netmask>：IP 的子网掩码。

缺省情况：缺省所有 IP 都为非信任 IP。掩码缺省为 255.255.255.255。

命令模式：全局配置模式。

使用指南：如果某 IP 被配置为信任 IP，则防 ARP 扫描功能将不对此 IP 作处理，即使从其收到的 ARP 报文速率超过了设定的阈值，也不禁掉此 IP。如果此 IP 已经被防 ARP 扫描禁掉，则立即恢复其流量。

举例：将 192.168.1.0/24 配置为信任 IP。

```
Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0
```

2.6 anti-arpscan recovery enable

命令：anti-arpscan recovery enable
no anti-arpscan recovery enable

功能：启动自动恢复功能，no 命令取消自动恢复功能。

参数：无。

缺省情况：关闭自动恢复功能。

命令模式：全局配置模式。

使用指南：如果希望端口被关闭一段时间后，自动恢复为正常状态，则可配置此功能。

举例：

在交换机上启动自动恢复功能。

```
Switch(config)#anti-arpscan recovery enable
```

2.7 anti-arpscan recovery time

命令：anti-arpscan recovery time <seconds>

no anti-arpscan recovery time

功能：配置自动恢复时间；no 命令恢复自动恢复时间为默认值。

参数：自动恢复时间值，单位为秒。有效范围为 5-86400 秒。

缺省情况：300 秒。

命令模式：全局配置模式。

使用指南：必须先启动自动恢复功能。

举例：设置自动恢复时间为 3600 秒。

```
Switch(config)#anti-arpscan recovery time 3600
```

2.8 anti-arpscan log enable

命令：anti-arpscan log enable

no anti-arpscan log enable

功能：启动防 ARP 扫描的日志功能；no 命令关闭防 ARP 扫描的日志功能。

参数：无。

缺省情况：关闭防 ARP 扫描的日志功能。

命令模式：全局配置模式。

使用指南：打开防 ARP 扫描的日志功能后，可以通过日志信息查看端口被防 ARP 扫描关闭及自动恢复、IP 被禁掉及被恢复的详细信息。日志的等级为 Warning。

举例：在交换机上启动防 ARP 扫描的日志功能。

```
Switch(config)#anti-arpscan log enable
```

2.9 anti-arpscan trap enable [level1|level2]

命令：anti-arpscan trap enable [level1|level2]

no anti-arpscan trap enable [level1|level2]

功能：启动防 ARP 扫描的 SNMP Trap 功能；no 命令关闭防 ARP 扫描的 SNMP Trap 功能。

参数：无。

缺省情况：缺省时为同时关闭或开启一级限速及二级隔离 trap 功能。

命令模式：全局配置模式。

使用指南：打开防 ARP 扫描的 SNMP Trap 功能后，在端口被防 ARP 扫描关闭或恢复，IP 被禁掉或恢复时，可通过网管软件收到 Trap 消息。

举例：在交换机上启动防 ARP 扫描的 SNMP Trap 功能。

Switch(config)#anti-arp scan trap enable level1

2.10 anti-arp scan ip-based level2 action {isolate | discard-ARP}

命令：anti-arp scan ip-based level2 action {isolate | discard-ARP}

功能：超过二级阈值后的处理动作可配置为 IP 业务隔离和丢弃 ARP 报文不送 CPU。

参数：isolate—该 IP 的业务被隔离，discard-ARP ---丢弃该 IP 上来的 ARP 报文，但保留其原 ARP 表项。默认动作为 discard-ARP。

命令模式：全局配置模式。

使用指南：配置超过二级阈值保护动作为 discard-arp，当某端口收到的以某一 IP 为源的 ARP 报文的速率大于二级阈值时，将此 IP 的 ARP 报文丢弃，IP 数据正常转发；配置超过二级阈值保护动作为 isolate，当某端口收到的以某一 IP 为源的 ARP 报文的速率大于二级阈值时，将此 IP 的 ARP 报文和 IP 数据都被丢弃。

举例：Switch(config)#anti-arp scan ip-based level2 action isolate

2.11 anti-arp scan FFP max-num <num>

命令：anti-arp scan FFP max-num <num>

功能：防 ARP 扫描功能可占用的 FFP 表项最大数量。

参数：<1-1024>，默认 200 个可用表项资源。

命令模式：全局配置模式。

使用指南：当端口收到的 arp 报文的源大于 max-num，且每个源 ip 的 arp 速率超过一级或者二级阈值，FFP 资源耗尽后，会提示资源不足，可适当将 ffp 表项的最大值调高。

举例：Switch(config)#anti-arp scan ffp max-num 1024

2.12 anti-arp scan ip-based arp-to-cpu speed<pps>

命令：anti-arp scan ip-based arp-to-cpu speed<pps>

no anti-arp scan ip-based arp-to-cpu speed

功能：配置一级阈值超限后 ARP 送 CPU 的速率。

参数：<1-20>，默认值为 1p/s。

命令模式：全局配置模式。

使用指南：用于配置 arp 速率超过一级限速后 arp 报文上 cpu 的速率，可以实时修改。

举例：Switch(config)#anti-arp scan ip-based arp-to-cpu speed 2

2.13 show anti-arp scan

命令：show anti-arp scan [trust {ip | port | supertrust-port | iptrust-port} | prohibited {ip | port}]

功能：显示防 ARP 扫描功能运行信息。

参数：无。

缺省情况：显示所有端口是否是信任端口，是否被关闭，如果被关闭了，则还显示被关闭了多长时间。显示所有的信任 IP，所有被禁掉的 IP。

命令模式：特权模式、配置模式。

使用指南：若只查看配置的信任端口则使用命令 `show anti-arpscan trust port`，如此类推。

举例：在交换机上启动防 ARP 扫描功能后查看运行情况。

Switch(config)#show anti-arpscan

Total port: 36

Name	Port-property	beShut	shutTime(seconds)
Ethernet1/1	untrust	N	0
Ethernet1/2	untrust	N	0
Ethernet1/3	untrust	N	0
Ethernet1/4	untrust	N	0
Ethernet1/5	untrust	N	0
Ethernet1/6	untrust	N	0
Ethernet1/7	untrust	N	0
Ethernet1/8	untrust	N	0
Ethernet1/9	untrust	N	0
Ethernet1/10	untrust	N	0
Ethernet1/11	untrust	N	0
Ethernet1/12	untrust	N	0
Ethernet4/1	untrust	N	0
Ethernet4/2	untrust	N	0
Ethernet4/3	untrust	N	0
Ethernet4/4	trust	N	0
Ethernet4/5	untrust	N	0
Ethernet4/6	supertrust	N	0
Ethernet4/7	untrust	Y	30
Ethernet4/8	trust	N	0
Ethernet4/9	untrust	N	0
Ethernet4/10	untrust	N	0
Ethernet4/11	untrust	N	0
Ethernet4/12	untrust	N	0
Ethernet4/13	untrust	N	0
Ethernet4/14	untrust	N	0
Ethernet4/15	untrust	N	0
Ethernet4/16	untrust	N	0
Ethernet4/17	untrust	N	0
Ethernet4/18	untrust	N	0
Ethernet4/19	untrust	N	0
Ethernet4/20	untrust	N	0
Ethernet4/21	untrust	N	0
Ethernet4/22	untrust	N	0

Ethernet4/23	untrust	N	0
Ethernet4/24	untrust	N	0

Prohibited IP:

IP	shutTime(seconds)
1.1.1.2	132

Trust IP:

192.168.99.5	255.255.255.255
192.168.99.6	255.255.255.255

2.14 show anti-arpscan ip-based attack-list [history]

命令：show anti-arpscan ip-based attack-list [history]

功能：显示防 ARP 扫描攻击源信息或历史攻击源信息。

参数：无。

缺省情况：显示防 ARP 扫描攻击源信息。

命令模式：特权模式、配置模式。

使用指南：

- 1) 显示防 arp 扫描攻击源信息，包括源 ip，对应端口，所属 vlan，速率，及状态。超过一级阈值的 state 为 Speed-Limit，超过二级阈值时，action 为 discard-arp 则 state 为 Discard-Arp，action 为 isolate 则 state 为 Isolate。
- 2) 显示防 arp 扫描历史攻击源信息，包括源 ip，对应端口，所属 vlan，攻击次数，最后一次攻击的状态，及攻击持续时间。超过一级阈值的 state 为 Speed-Limit，超过二级阈值时，action 为 discard-arp 则 state 为 Discard-Arp，action 为 isolate 则 state 为 Isolate。

举例：

Switch#show anti-arpscan ip-based attack-list

SIP-Addr	Port	VLAN	Speed	ARP-Count
State				
30.1.1.6	Ethernet2/48	26	4	57
Speed-Limit				
30.1.1.4	Ethernet2/48	26	4	56
Speed-Limit				

Switch#show anti-arpscan ip-based attack-list history

SIP-Addr	Port	VLAN	Attack-Times	State
Keep-Time				
30.1.1.6	Ethernet2/48	26	6	Speed-Limit
0 weeks,0 days,0 hours,8 minutes,46 seconds				
30.1.1.4	Ethernet2/48	26	3	Speed-Limit
0 weeks,0 days,0 hours,0 minutes,28 seconds				

2.15 show anti-arpscan ip-based running-config

命令：show anti-arpscan ip-based running-config

功能：显示防 arp 扫描的当前配置。

参数：无。

命令模式：特权模式、配置模式。

使用指南：显示当前防 arp 扫描的相关配置，如果一级、二级阈值，超过二级阈值后采用的动作，arp 超过一级阈值后上 cpu 的速率，ffp 表项大小等。

举例：

Switch(config)#show anti-arpscan ip-based running-config

level1 thrshould: 4

level2 thrshould: 8

level2 action: Discard-Arp

arp-to-cpu speed: 2

actIp-num: 0

ffp-max: 1024

ffp-used: 0

2.16 clear anti-arpscan speed-limit< IP Address>

命令：clear anti-arpscan speed-limit< IP Address>

功能：手动清除对特定主机的 ARP 限速。

参数：特定主机的 IP 地址。

命令模式：特权模式。

使用指南：当 arp 报文超过一级限速时，可以通过该命令清除表项，能够通过打开 debug 命令 debug anti-arpscan ip 查看表项被删除。

举例：Switch#clear anti-arpscan speed-limit 30.1.1.6

2.17 clear anti-arpscan ip-isolate <IP Address>

命令：clear anti-arpscan ip-isolate <IP Address>

功能：手动清除对特定主机的 IP 业务隔离。

参数：特定主机的 IP 地址。

命令模式：特权模式。

使用指南：当 arp 报文超过二级限速时，可以通过该命令清除表项，能够通过打开 debug 命令 debug anti-arpscan ip 查看表项被删除。

举例：Switch#clear anti-arpscan ip-isolate 30.1.1.6

2.18 clear anti-arpscan attack-list {ip <IP Address>| all}

命令：clear anti-arpscan attack-list {ip <IP Address> | all}

功能：手动清除对特定主机或所有主机的限制。

参数：<IP Address>：特定主机的 IP 地址。

命令模式：特权模式。

使用指南：当 arp 报文超过一级或二级限速时，可以通过该命令清除表项，能够通过打开 debug 命令 debug anti-arpscan ip 查看表项被删除。

举例：Switch#clear anti-arpscan attack-list ip 30.1.1.6

2.19 clear anti-arpscan attack-history-list {ip <IP Address>| all}

命令：clear anti-arpscan attack-history-list {ip <IP Address> | all}

功能：手动清除特定主机或所有主机的攻击历史信息。

参数：<IP Address>：特定主机的 IP 地址。

命令模式：特权模式。

使用指南：可以通过该命令清除攻击的历史信息，可以通过命令 show anti-arpscan ip-based attack-list history 查看表项被删除。

举例：Switch#clear anti-arpscan attack-history-list ip 30.1.1.6

2.20 debug anti-arpscan

命令：debug anti-arpscan [port | ip]

no debug anti-arpscan [port | ip]

功能：打开防 ARP 扫描的调试开关；no 命令关闭防 ARP 扫描的调试开关。

参数：无。

缺省情况：关闭防 ARP 扫描的调试开关。

命令模式：特权模式。

使用指南：打开防 ARP 扫描的调试开关后，在端口被防 ARP 扫描关闭，或端口自动恢复，IP 被禁掉或恢复时，可查看相应的调试信息。也可单独打开基于端口或基于 IP 的调试开关。

举例：在交换机上打开防 ARP 扫描的调试开关。

Switch#debug anti-arpscan

第3章 ARP、ND绑定配置命令

3.1 ip arp-security updateprotect

命令： ip arp-security updateprotect
no ip arp-security updateprotect

功能： 禁止 IPv4 版本的 ARP 更新功能，no 命令操作重新启动 ARP 更新功能。

参数： 无

缺省情况： 学习 ARP 并正常更新。

命令模式： 全局配置模式/接口配置。

使用指南： 本命令用于防止 ARP 的 request 和 reply 报文对交换机进行 ARP 表的更新操作。不过即使在不转换动态 ARP 的情况下，如果交换机一直收到合法的 ARP 请求/应答报文则此动态表项不会超时，当收到的 ARP 请求或应答包与保存不符才予以丢弃。命令全局优先。此功能与 I3 station move 功能互斥，I3 station move 功能会自动更新 ARP 的 MAC 和端口的对应关系（此功能默认是开启的），所以使能 ARP 安全更新功能的同时需要关闭 I3 station move 功能。

举例：

```
Switch(Config-if-Vlan1)#ip arp-security updateprotect
Switch(config)#ip arp-security updateprotect
```

3.2 ipv6 nd-security updateprotect

命令： ipv6 nd-security updateprotect
no ipv6 nd-security updateprotect

功能： 禁止 IPv6 版本的 ND 更新功能，no 命令操作重新启动 ND 更新功能。

参数： 无。

缺省情况： 学习 ND 并正常更新。

命令模式： 全局配置模式/接口配置。

使用指南： 本命令用于防止 ND 的 request 和 reply 报文对交换机进行 ND 表的更新操作。不过即使在不转换动态 ND 的情况下，如果交换机一直收到合法的 ND 请求/应答报文则此动态表项不会超时，当收到的 ND 请求或应答包与保存不符才予以丢弃。命令全局优先。

举例：

```
Switch(Config-if-Vlan1)#ipv6 nd-security updateprotect
Switch(config)#ipv6 nd-security updateprotect
```

3.3 ip arp-security learnprotect

命令： ip arp-security learnprotect
no ip arp-security learnprotect

功能： 禁止 IPv4 版本的 ARP 自动学习功能，no 命令操作重新启动 ARP 自动学习功能。

参数：无。

缺省情况：学习 ARP 并正常更新。

命令模式：全局配置模式/接口配置。

使用指南：本命令用于在防止 ARP 的自动学习与更新。与 ip arp-security updateprotect 不同的是，此命令开启后，无论是否合法的 ARP 表项，即使一直发送请求/应答报文，一样会超时。建议与转换操作搭配使用，命令全局优先。

举例：

```
Switch(Config-if-Vlan1)#ip arp-security learnprotect
```

```
Switch(config)#ip arp-security learnprotect
```

3.4 ipv6 nd-security learnprotect

命令：ipv6 nd-security learnprotect

no ipv6 nd-security learnprotect

功能：禁止 IPv6 版本的 ND 自动学习功能，no 命令操作重新启动 ND 自动学习功能。

参数：无。

缺省情况：学习 ND 并正常更新。

命令模式：全局配置模式/接口配置。

使用指南：本命令用于在防止 ND 的自动学习与更新。与 ip nd-security updateprotect 不同的是，此命令开启后，无论是否合法的 ND 表项，即使一直发送请求/应答报文，一样会超时。建议与转换操作搭配使用，命令全局优先。

举例：

```
Switch(Config-if-Vlan1)#ipv6 nd-security learnprotect
```

```
Switch(config)#ipv6 nd-security learnprotect
```

3.5 ip arp-security convert

命令：ip arp-security convert

功能：将所有动态 ARP 转变为静态 ARP。

参数：无。

命令模式：全局配置模式/接口配置。

使用指南：本命令用于将动态 ARP 表项转换为静态的 ARP 表项。配合关闭学习功能达到防止 ARP 绑定的作用。执行之后，该命令就无效了。

举例：

```
Switch(Config-if-Vlan1)#ip arp-security convert
```

```
Switch(config)# ip arp-security convert
```

3.6 ipv6 nd-security convert

命令：ipv6 nd-security convert

功能：将所有动态 ND 转变为静态 ND。

参数：无。

命令模式： 全局配置模式/接口配置。

使用指南： 本命令用于将动态 ND 表项转换为静态的 ND 表项。配合关闭学习功能达到防止 ND 绑定的作用。执行之后，该命令就无效了。

举例：

```
Switch(Config-if-Vlan1)#ipv6 nd-security convert  
Switch(config)#ipv6 nd-security convert
```

3.7 clear ip arp dynamic

命令： clear ip arp dynamic

功能： 清除接口上所有的动态 ARP。

参数： 无。

命令模式： 接口配置。

使用指南： 本命令用于在使用 ARP 绑定功能之前的动态表项清理工作。执行之后，该命令就无效了。

举例：

```
Switch(Config-if-Vlan1)#clear ip arp dynamic
```

3.8 clear ipv6 nd dynamic

命令： clear ipv6 nd dynamic

功能： 清除接口上所有的动态 ND。

参数： 无。

命令模式： 接口配置。

使用指南： 本命令用于在使用防 ND 绑定功能之前的动态表项清理工作。执行之后，该命令就无效了。

举例：

```
Switch(Config-if-Vlan1)#clear ipv6 nd dynamic
```

第4章 ARP GUARD配置命令

4.1 arp-guard ip

命令：arp-guard ip <addr>

no arp-guard ip <addr>

功能：添加 ARP GUARD 地址，no 命令操作删除 ARP GUARD 地址。

参数：<addr>：受到保护的 IP 地址，点分十进制形式。

缺省情况：默认没有 ARP GUARD 地址。

命令模式：端口配置模式。

使用指南：配置 ARP GUARD 地址之后，从配置了 ARP GUARD 的端口接收到的 ARP 报文将被进行过滤，如果 ARP 报文的源 IP 地址匹配该端口上所配置 ARP GUARD 地址，就认为是 ARP 欺骗攻击报文，这样的 ARP 报文将直接被丢弃，不会送交换机 CPU，也不会被转发，每个端口下最多可以配置 16 个 ARP GUARD 地址。

举例：

在端口 Ethernet1/1 启动配置 ARP GUARD 地址 100.1.1.1。

```
Switch(config)#interface ethernet1/1
```

```
Switch(Config-If-Ethernet1/1)#arp-guard ip 100.1.1.1
```

在端口 Ethernet1/1 删除 ARP GUARD 地址 100.1.1.1。

```
Switch(config)#interface ethernet1/1
```

```
Switch(Config-If-Ethernet1/1)#no arp-guard ip 100.1.1.1
```

第5章 Arp local proxy命令

5.1 ip local proxy-arp

命令：ip local proxy-arp

no ip local proxy-arp

功能：打开/关闭指定接口的 local arp proxy 功能。

参数：无。

缺省情况：所有的接口默认不启动此功能。

命令模式：VLAN 接口配置模式。

使用指南：打开接口的 local arp proxy 功能后，对于从本接口收到的 arp request 报文，如果 arp request 报文中的目的 ip 和源 ip 都与该接口的 ip 处于同一网段，则交换机会回应 arp reply 报文，将交换机的 mac 填充到 arp REPLY 报文中。用这种方式来引导所有的 ip 流量通过交换机进行三层转发。

举例：打开 Vlan1 接口的 local arp proxy 功能。

Switch(Config-if-Vlan1)#ip local proxy-arp

第6章 免费ARP发送功能配置命令

6.1 ip gratuitous-arp

命令：ip gratuitous-arp [*<interval-time>*]

no ip gratuitous-arp

功能：使能免费 ARP 发送功能，并设置发送免费 ARP 报文的间隔时间；本命令的 no 命令为取消使能免费 ARP 发送功能。

参数：*<interval-time>* 为发送免费 ARP 报文的间隔时间；范围为 5-1200 秒，默认为 300 秒。

命令模式：全局配置模式和接口配置模式。

缺省情况：不使能免费 ARP 发送功能。

使用指南：在全局配置模式下使能免费 ARP 发送功能时，将使能系统中所有存在的三层接口的免费 ARP 发送功能。在接口配置模式下使能免费 ARP 发送功能时，只是使能当前接口的免费 ARP 发送功能。配置的免费 ARP 发送间隔时间以接口配置模式下配置的间隔时间为准。如果全局配置模式下和接口配置模式下都配置了免费 ARP 发送功能的发送间隔时间时，使用接口配置模式下配置的间隔时间。

举例：

1) 全局配置模式下使能免费 ARP 发送功能，并设置免费 ARP 发送间隔时间为 400 秒。

```
Switch>enable
```

```
Switch#config
```

```
Switch(config)#ip gratuitous-arp 400
```

2) 接口配置模式下使能接口 interface vlan 10 的免费 ARP 发送功能，并设置免费 ARP 发送间隔时间为 350 秒。

```
Switch(config)#interface vlan 10
```

```
Switch(Config-if-Vlan10)#ip gratuitous-arp 350
```

6.2 show ip gratuitous-arp

命令：show ip gratuitous-arp [interface vlan *<vlan-id>*]

功能：显示免费 ARP 发送功能的配置信息。

参数：*<vlan-id>*：为指定的 VLAN 号。*<vlan-id>*的取值范围为 1 ~ 4094。

命令模式：各种配置模式。

使用指南：在任意命令模式下，输入命令 **show ip gratuitous-arp**，则显示全局配置模式下和接口配置模式下的免费 ARP 发送功能配置信息。如果输入命令 **show ip gratuitous-arp interface vlan *<vlan-id>***，则显示指定接口的免费 ARP 发送功能配置信息。

举例：

1) 显示全局配置模式下和接口配置模式下的免费 ARP 发送功能配置信息。

```
Switch#show ip gratuitous-arp
```

```
Gratuitous ARP send is Global enabled, Interval-Time is 300(s)
```

Gratuitous ARP send enabled interface vlan information:

Name	Interval-Time(seconds)
Vlan1	400
Vlan10	350

2) 显示接口 interface vlan 10 的免费 ARP 发送功能配置信息。

Switch#show ip gratuitous-arp interface vlan 10

Gratuitous ARP send interface Vlan10 information:

Name	Interval-Time(seconds)
Vlan10	350

第7章 Keepalive gateway配置命令

7.1 keepalive gateway

命令： `keepalive gateway <ip-address> [{<interval-seconds> | msec <interval-millisecond>} [retry-count]]`

no keepalive gateway

功能： 启动 keepalive gateway 功能和配置发送 ARP 请求报文的间隔周期和判定探测失败的重试次数，no 命令为关闭该功能。

参数： ip-address 为探测的网关 IP 地址。

interval-seconds: 发送 ARP 请求报文的间隔周期（秒），取值范围：1-32767。如果不配置，缺省是 10 秒。

interval-millisecond: 发送 ARP 请求报文的间隔周期（毫秒），取值范围：160-999。

retry-count: 判定探测失败的重试次数。如果不配置，缺省是 5 次。

缺省情况： 默认关闭 keepalive gateway 功能。

命令模式： 接口配置模式

使用指南： 只在三层交换机上才具有该命令，二层交换机上不支持，该种探测方法仅适用于点对点的拓扑模式。

举例：

Switch(config)#interface vlan 1

Switch(config-if-vlan1)#keealive gateway 1.1.1.1 3 10

7.2 show ip interface

命令： `show ip interface [interface-name]`

功能： 显示指定接口的 IPv4 运行状态。

参数： interface-name 为指定接口名，如果参数为空，则显示所有接口的 IPv4 运行状态。

缺省情况： 无。

命令模式： 特权和配置模式

使用指南： 显示接口 IPv4 运行状态。

举例：

Switch(config)#show ip interface brief

Index	Interface	IP-Address	Protocol
3001	Vlan1	1.1.1.2	up
9000	Loopback	127.0.0.1	up

7.3 show keepalive gateway

命令： `show keepalive gateway [interface-name]`

功能：显示指定接口的 keepalive 运行情况。

参数：interface-name 为指定接口名，如果参数为空，则显示所有接口的 keepalive 运行状态。

缺省情况：无。

命令模式：特权和配置模式

使用指南：显示接口 keepalive 运行状态。

举例：

```
Switch(config)#show keepalive gateway
```

```
interface Vlan1 gateway 1.1.1.1 time 10s retry 1 remain 4 now UP
```

第8章 UFT配置命令

8.1 Show system working mode

命令： `show system working mode {support|current|config} {member<member-id>|} {slot<slot-id>|}`

功能： 显示板卡可以配置的 UFT 模式以及各个模式对应的表项大小

参数： support: 显示板卡支持的各种模式下表项大小

current: 显示当前各板卡生效的模式及表项大小

config: 显示各板卡配置的模式及表项大小

member: 堆叠模式成员编号

slot: 机架设备线卡槽位号

缺省情况： 无

命令模式： 全局配置模式

使用指南： member 作为可选项，如果是独立模式，不需要输入 member。如果是机架式设备可以对指定槽位的线卡进行 UFT 表项大小查看。

举例：

查看线卡 2 当前配置的 UFT 模式和当前生效的 UFT 模式

Switch#show system working mode config slot 2

-----slot: 2 -----

config system working mode: mode 1(bridgee)

mode 1(bridgee): MAC=288K, IP=16K, ROUTER=8K

Switch#show system working mode current slot 2

-----slot: 2 -----

current system working mode: mode 1(bridgee)

mode 1(bridgee): MAC=288K, IP=16K, ROUTER=8K

8.2 System working mode

命 令： `system working mode {bridgee|routee|standard|<word>} {member<member-id>|} {slot<slot-id>|}`

功能： 按照用户业务需要设置 UFT 工作模式，需要重启线卡后生效。

参数： bridgee: 增强 mac 模式

routee: 增强路由模式（路由条目数暂不支持 128K）

standard: 标准模式

member: 堆叠模式成员编号

slot: 机架设备线卡槽位号

不同的板卡各模式支持的表项是不一样的，可以通过命令 `show system working mode support` 查看：

-----slot: 1 -----

current system support mode:

mode 1(bridgee): MAC=288K, IP=16K, ROUTER=8K

```
mode 2(routee): MAC=32K, IP=16K, ROUTER=128K
mode 3(standard): MAC=96K, IP=208K, ROUTER=8K
mode 4: MAC=160K, IP=144K, ROUTER=8K
mode 5: MAC=224K, IP=80K, ROUTER=8K
-----slot: 2 -----
mode 1(bridgee): MAC=304K, IP=112K, ROUTER=8K
mode 2(routee): MAC=112K, IP=304K, ROUTER=8K
mode 3(standard): MAC=112K, IP=304K, ROUTER=8K
mode 4: MAC=208K, IP=208K, ROUTER=8K
mode 5: MAC=400K, IP=16K, ROUTER=8K
```

缺省情况： 默认线卡工作在 standard 模式。

命令模式： 全局配置模式

使用指南： member 作为可选项，如果是独立模式，不需要输入 member。如果是机架式设备可以对指定槽位的线卡进行 UFT 工作模式设置。更改 UFT 工作模式后，要求重启相应线卡才能生效。

举例：

修改线卡 2 的 UFT 工作模式

```
Switch(config)#system working mode bridgee slot 2
```

Please save the configuration, it will take effect after the next system restart!

保存配置，重启线卡 2

```
Switch#write
```

Confirm to overwrite current startup-config configuration [Y/N]:y

Write running-config to current startup-config successful

```
Switch#reset slot 2
```