三层管理分册

目录

三层管理分册.....1

目录.....1

1 手册说明.....10

1.1 手册说明简介.....10

1.2 命令行格式约定.....**错误！未定义书签。**

1.3 命令行模式说明.....**错误！未定义书签。**

1.3.1 enable.....**错误！未定义书签。**

1.3.2 disable.....**错误！未定义书签。**

1.3.3 exit.....**错误！未定义书签。**

1.3.4 end.....**错误！未定义书签。**

1.3.5 list.....**错误！未定义书签。**

1.3.6 configure terminal.....**错误！未定义书签。**

1.3.7 terminal length.....**错误！未定义书签。**

1.3.8 idle-timeout.....**错误！未定义书签。**

2 配置三层接口.....10

2.1 三层接口简介.....13

2.2 创建删除三层接口.....13

2.2.1 interface IFNAME.....13

2.2.2 no interface IFNAME.....14

2.3 配置三层接口.....15

2.3.1 ip address.....15

2.3.2 no ip address.....15

2.3.3 ipv6 address.....15

2.3.4 no ipv6 address.....16

2.3.5 shutdown.....16

2.3.6 no shutdown.....16

2.3.7 advanced-routing....16
2.3.8 link-detect....17
2.3.9 config qinq-type VALUE....17
2.3.10 add|delete bonding interface....18
2.3.11 set mode....18
2.4 显示三层接口信息....19
2.4.1 show interface....19
2.4.2 show bonding BONDX....20
3 配置 ARP....20
3.1 ARP 功能简介....20
3.2 配置 ARP....20
3.2.1 ip static-arp....20
3.2.2 no ip static-arp....21
3.2.3 add|del arp IP MAC base IFNAME....22
3.2.4 config arp smac-check....22
3.2.5 clear eth-port arp....23
3.2.6 clear trunk arp....23
3.3 显示 ARP 信息....24
3.3.1 show arp list....24
3.3.2 show arp by interface....24
3.3.3 show arp by ip....24
3.3.4 show arp by mac....25
3.3.5 show arp by state....25
3.3.6 show eth-port arp....25
3.3.7 show trunk arp....26
4 配置 DHCP server....26
4.1 DHCP server 功能简介....26
4.2 配置 DHCP server 全局参数....26
4.2.1 ip dhcp server enable|disable....26
4.2.2 ip dhcp server domain....27

4.2.3 ip dhcp server dns....27
4.2.4 ip dhcp server wins....28
4.2.5 ip dhcp server lease-default....28
4.2.6 ip dhcp server lease-time....29
4.2.7 ip dhcp static....29
4.2.8 ip dhcp reply-mode....30
4.3 配置 DHCP server 的 IP 地址池....30
4.3.1 ip pool....30
4.3.2 no ip pool....30
4.3.3 config ip pool....31
4.3.4 add|delete range....31
4.3.5 ip dhcp server dns....32
4.3.6 ip dhcp server wins....32
4.3.7 ip dhcp server lease-default....33
4.3.8 ip dhcp server lease-time....33
4.3.9 ip dhcp server domain....33
4.3.10 ip dhcp server option43....34
4.3.11 ip dhcp server option138....34
4.4 配置三层接口绑定 IP 地址池....35
4.4.1 ip pool....35
4.5 显示 DHCP server 配置信息....36
4.5.1 show ip dhcp....36
4.5.2 show ip pool....36
4.5.3 show ip dhcp static....36
4.5.4 show dhcp-lease....36
5 配置 DHCP ipv6 server....**错误！未定义书签。**
5.1 DHCP ipv6 server 功能简介....**错误！未定义书签。**
5.2 配置 DHCP ipv6 server 全局参数....**错误！未定义书签。**
5.2.1 ipv6 dhcp server domain-search....**错误！未定义书签。**
5.2.2 ipv6 dhcp server name-servers....**错误！未定义书签。**

5.2.3 ipv6 dhcp server lease-default ..... **错误！未定义书签。**
5.2.4 ipv6 dhcp server lease-time ..... **错误！未定义书签。**
5.3 配置 DHCP Ipv6 server 的 ipv6 地址池 ..... **错误！未定义书签。**
5.3.1 ipv6 pool ..... **错误！未定义书签。**
5.3.2 config ipv6 pool ..... **错误！未定义书签。**
5.3.3 add|delete rangev6 ..... **错误！未定义书签。**
5.3.4 ipv6 dhcp server domain-search ..... **错误！未定义书签。**
5.3.5 ipv6 dhcp server name-servers ..... **错误！未定义书签。**
5.3.6 ipv6 dhcp server lease-default ..... **错误！未定义书签。**
5.3.7 ipv6 dhcp server lease-time ..... **错误！未定义书签。**
5.4 配置三层接口绑定 ipv6 地址池 ..... **错误！未定义书签。**
5.4.1 ipv6 pool ..... **错误！未定义书签。**
5.5 显示 DHCP ipv6 server 配置信息 ..... **错误！未定义书签。**
5.5.1 show ipv6 dhcp ..... **错误！未定义书签。**
5.5.2 show ipv6 pool ..... **错误！未定义书签。**
5.5.3 show dhcp-lease-ipv6 ..... **错误！未定义书签。**
6 配置 DHCP Relay 37
6.1 DHCP Relay 功能简介 37
6.2 配置 DHCP Relay 37
6.2.1 ip dhcp relay enable|disable 37
6.2.2 ip relay IFNAME 37
6.2.3 no ip relay IFNAME 38
6.3 显示 DHCP Relay 配置 38
6.3.1 show ip dhcp relay 38
7 配置 DHCP Snooping 38
7.1 DHCP Snooping 功能简介 38
7.2 配置 LAN 模式全局 DHCP Snooping 39
7.2.1 config dhcp-snooping lan enable|disable 39
7.2.2 config dhcp-snooping information enable|disable 39
7.2.3 config dhcp-snooping information format 40

7.2.4 config dhcp-snooping information packet-format....40
7.2.5 config dhcp-snooping information remote-id....41
7.2.6 dhcp-snooping static-binding ip-address....41
7.3 配置 LAN 模式 VLAN 节点下的 DHCP Snooping....42
7.3.1 config dhcp-snooping enable|disable....42
7.3.2 config dhcp-snooping PORTNO mode....43
7.3.3 config dhcp-snooping information strategy PORTNO ploicy....44
7.3.4 config dhcp-snooping information circuit-id PORTNO content....44
7.3.5 config dhcp-snooping information remote-id PORTNO content....45
7.4 配置 WAN 模式全局 DHCP Snooping....46
7.4.1 config dhcp-snooping wan enable|disable....46
7.4.2 config dhcp-snooping IFNAME enable|disable....46
7.4.3 set dhcp-snooping-wan static arp op enable|disable....**错误！未定义书签。**
7.5 配置 WAN 模式接口节点下的 DHCP Snooping....47
7.5.1 config dhcp-snooping enable|disable....47
7.6 显示 DHCP Snooping 配置信息....47
7.6.1 show dhcp-snooping....47
7.6.2 show dhcp-snooping trust....48
7.6.3 show dhcp-snooping static-binding....48
7.6.4 show dhcp-snooping static-binding vlan....48
7.6.5 show dhcp-snooping static-binding eth-port PORTNO....48
8 配置 IGMP Snooping....49
8.1 IGMP Snooping 功能简介....49
8.2 配置全局 IGMP Snooping....49
8.2.1 config igmp-snooping enable|disable....49
8.2.2 config igmp-snooping timeout....50
8.3 配置 vlan 节点下的 IGMP Snooping....50
8.3.1 config igmp-snooping enable|disable....50
8.3.2 config igmp-snooping PORTNO enable|disable....51
8.3.3 add|delete igmp-snooping route-port PORTNO....51

8.4 显示 IGMP Snooping 配置.....52
8.4.1 show igmp-snooping time.....52
8.4.2 show igmp-snooping vlan-count.....52
8.4.3 show igmp-snooping vlan-list.....52
8.4.4 show igmp-snooping group-count.....53
8.4.5 show igmp-snooping group-list vlan.....53
8.4.6 show igmp-snooping route-port vlan.....53
8.4.7 show multicast-group count.....54
8.4.8 show multicast-group list.....54
8.4.9 show multicast-group route-port.....54
9 配置 ACL.....54
9.1 ACL 功能简介.....55
9.2 配置 ACL.....55
9.2.1 config acl service.....55
9.2.2 Acl ip (permit|deny| trap).....55
9.2.3 Acl ip redirect.....56
9.2.4 Acl (tcp | udp) (permit | deny | trap).....57
9.2.5 Acl (tcp | udp) redirect.....57
9.2.6 Acl icmp (permit | deny | trap).....58
9.2.7 Acl icmp redirect.....59
9.2.8 Acl arp (permit | deny | trap).....59
9.2.9 Acl arp(redirect| mirror).....60
9.2.10 Acl Ethernet (permit | deny | trap).....60
9.2.11 Acl Ethernet redirect.....61
9.2.12 Extended acl(tcp|udp)(permit | deny| trap).....62
9.2.13 Extended acl(tcp|udp)redirect.....62
9.2.14 Acl Ethertype (permit | deny | trap).....63
9.2.15 Acl Ethertype redirect.....64
9.2.16 Acl ipv6 tcp|udp (permit | deny | trap).....64
9.2.17 delete acl.....65

9.2.18 create acl-group 66
9.2.19 config acl-group 66
9.2.20 add/delete acl 66
9.2.21 add/delete acl-range 67
9.2.22 acl (enable|disable) 67
9.2.23 acl-range standard ip 68
9.2.24 acl ingress-qos 68
9.2.25 acl egress–qos 69
9.2.26 append acl 70
9.2.27 delete append 70
9.2.28 bind/unbind acl-group 70
9.3 显示 ACL 71
9.3.1 show acl service 71
9.3.2 show acl list 71
9.3.3 show acl 71
9.3.4 show acl-group 72
10 配置 Firewall 和 NAT 72
10.1 Firewall 和 NAT 功能简介 72
10.2 配置 Firewall 和 NAT 72
10.2.1 config firewall 72
10.2.2 add (firewall|snat|input) desc 73
10.2.3 add dnat desc DESC nat-ip 73
10.2.4 del (firewall|snat|dnat|input) 74
10.2.5 change (firewall|snat|dnat|input) INDEX index 74
10.2.6 modify (firewall|snat|dnat|input) INDEX desc 74
10.2.7 modify (firewall|snat|dnat|input) INDEX valid 75
10.2.8 modify firewall INDEX (in-if|out-if) 75
10.2.9 modify (dnat|input) INDEX in-if 76
10.2.10 modify snat INDEX out-if 76
10.2.11 modify (firewall|snat|dnat|input) INDEX (src-ip|dst-ip) 76

10.2.12 modify (firewall|snat|dnat|input) INDEX protocol....77
10.2.13 modify (firewall|snat|dnat|input) INDEX (src-port|dst-port)....77
10.2.14 modify (firewall|input) INDEX state....78
10.2.15 modify (firewall|input) INDEX filter-string....79
10.2.16 modify (firewall|input) INDEX act....79
10.2.17 modify firewall INDEX act tcpmss....79
10.2.18 modify snat INDEX nat-ip any....80
10.2.19 modify (snat|dnat) INDEX nat-ip....80
10.2.20 modify (snat|dnat) INDEX nat-port....80
10.3 显示 Firewall 和 NAT 配置....81
10.3.1 show (firewall|snat|dnat|input)....81
10.3.2 show firewall-state....81
11 配置 QOS....82
11.1 QOS 功能简介....82
11.2 配置 QOS profile....82
11.2.1 config qos-mode....82
11.2.2 set qos-profile....83
11.2.3 qos-profile attributes....83
11.2.4 delete qos-profile....83
11.2.5 up-qos-profile mapping....84
11.2.6 delete up-qos-profile mapping....84
11.2.7 dscp-qos-profile mapping....84
11.2.8 delete dscp-qos-profile mapping....85
11.2.9 dscp-dscp remapping....85
11.2.10 delete dscp-dscp remapping....85
11.2.11 show qos-profile....86
11.2.12 show qos-mode....86
11.2.13 show remap-table....86
11.3 配置 policy-map....86
11.3.1 create policy-map....86

11.3.2 delete policy-map 87
11.3.3 config policy-map 87
11.3.4 config qos-markers 87
11.3.5 trust-mode layer2 88
11.3.6 trust-mode layer3 88
11.3.7 trust-mode layer2+layer3 89
11.3.8 show policy-map 89
11.4 绑定端口的 policy map 89
11.4.1 bind policy map 89
11.4.2 unbind policy map 90
11.4.3 show port-qos 90
11.5 配置流量监管 90
11.5.1 set policer 90
11.5.2 policer CIR CBS 91
11.5.3 config out profile 91
11.5.4 keep 91
11.5.5 drop 91
11.5.6 remap 92
11.5.7 strict mode 92
11.5.8 loose mode 92
11.5.9 enable policer 93
11.5.10 policer-range 93
11.5.11 delete policer 93
11.5.12 delete policer-range 94
11.5.13 show policer 94
11.6 配置流量整形 94
11.6.1 traffic-shape MAXRATE 94
11.6.2 delete traffic-shape port 95
11.6.3 traffic-shape queue <0-7> MAXRATE 95
11.6.4 delete traffic-shape queue 95

11.6.5 show traffic-shape 96
11.7 配置队列调度算法 96
11.7.1 queue-scheduler sp 97
11.7.2 queue-scheduler wrr 97
11.7.3 queue-scheduler hybrid 97
11.7.4 wrr (group1|group2) <0-7> <1-255> sp 97
11.7.5 show queue-scheduler 98

1 手册说明

1.1手册说明简介

AuteWareOS 命令行配置手册，一共分为六大部分，本文是第三部分三层管理分册。本章描述 AuteWareOS 命令行配置手册命令行格式约定，命令行配置的几种模式。

1.2命令行格式约定

格式	意义
大写	命令行中参数用大写表示，命令中必须由实际值进行替换。
[]	表示用“[]”括起来的部分配置时可选。
〈x-y〉	表示从 x-y 数值范围内选择一个作为参数。
（x|y|…）	表示从多个选项中仅选择一个作为参数。

1.3命令行模式说明

命令行模式分为视图模式、系统模式、配置模式和节点配置模式四种。

命令行模式	命令行显示	进入方式	可执行操作
视图模式	SYSTEM>	管理员通过串口\telnet\ssh 方式登陆设备	执行视图模式下的显示命令查看基本信息
系统模式	SYSTEM#	在视图模式下输入命令 enable	执行系统模式下的显示命令查看系统信息和执行设置命令对系统进行设置
配置模式	SYSTEM(config)#	在系统模式下输入命令 configure terminal	执行配置模式下的显示命令查看配置信

			息，执行设置命令设置全局参数，以及进入各配置节点
节点配置模式	显示节点配置，如： SYSTEM(config-vlan)#	在配置模式下输入进入相应节点的命令，如： config vlan 2	执行节点配置命令对节点进行配置，执行显示命令显示节点信息

四种模式层层递进关系，由浅入深，在深一层的模式下输入 exit 或者 quit 命令可以退出该模式，回到上层模式，输入 end 命令直接退到系统模式。进入系统模式或者更深层次后只能回退到系统模式，在系统模式下输入 exit 或者 quit 命令会断开与设备的连接。显示时 SYSTEM 为系统名称，有些设备名称更改过会显示不同。

四种模式切换的常用命令如下：

1.3.1 **enable**

【命令格式】 enable
【命令功能】 进入配置模式（节点）
【命令模式】 视图模式
【参数说明】 无
【默认状态】 无
【使用指导】 执行权限为管理员权限
【配置实例】 enable

1.3.2 **disable**

【命令格式】 disable
【命令功能】 退出当前系统模式，返回到视图模式。
【命令模式】 系统模式
【参数说明】 无
【默认状态】 无
【使用指导】 在系统模式下，执行 disable，返回到视图模式。
【配置实例】 disable

1.3.3 **exit**

【命令格式】 exit
quit
【命令功能】 退出当前配置模式，返回到上一级配置模式。
【命令模式】 任意模式
【参数说明】 无
【默认状态】 无
【使用指导】 在系统模式下，输入 exit 直接退出命令行模式，再次进入，需要重新登录。

【配置实例】 exit

1.3.4 **end**

【命令格式】 end
【命令功能】 退出当前模式到系统模式。
【命令模式】 配置模式、节点配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 在配置模式及节点配置模式下，执行 end，推出当前模式到系统模式。
【配置实例】 end

1.3.5 **list**

【命令格式】 list
【命令功能】 显示当前模式下所有命令集合
【命令模式】 任意模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
【配置实例】 list

1.3.6 **configure terminal**

【命令格式】 configure terminal
【命令功能】 进入配置模式
【命令模式】 系统模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
【配置实例】 configure terminal

1.3.7 **idle-timeout**

【命令格式】 idle-timeout <0-3600>
【命令功能】 设置用户登录的空闲时间
【命令模式】 系统模式、配置模式
【参数说明】

参数	说明
<0-3600>	设置老化时间的值，单位为分钟

【默认状态】 10 分钟
【使用指导】 用户登录后，如果达到空闲时间没有任何输入，将自动退出登录
【配置实例】 idle-timeout 30

1.3.8 no idle-timeout

【命令格式】 no idle-timeout
【命令功能】 取消设置用户登录的空闲时间
【命令模式】 系统模式、配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
【配置实例】 no idle-timeout

1.3.9 show idle-timeout

【命令格式】 show idle-timeout
【命令功能】 显示设置用户登录的空闲时间值
【命令模式】 视图模式、系统模式、配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
【配置实例】 show idle-timeout

2 配置三层接口

2.1三层接口简介

三层接口指设备中的运行于网络层的接口，包括 vlan 三层接口、以太网三层接口、以太网三层子接口和以太网三层 qinq 子接口。

bond 接口是将多个接口绑定成一个独立的接口，使得被绑定的接口之间可以进行备份，也可以进行负载均衡。我们现在支持创建 8 个 bond 接口，分别对应 bond0～bond7。创建后的 bonding 接口，等同于其他的三层接口，可以 interface 这个接口后进行配置，添加删除绑定的接口，配置 ip 等操作。

2.2 创建删除三层接口

2.2.1 interface IFNAME

【命令格式】 interface IFNAME
【命令功能】 根据接口名不同创建不同类型接口，并进入接口模式，

接口包括 VLAN+ID 接口，Eth 接口，Eth 子接口，Eth qinq 子接口，Bond+ID 接口，Bond+id 子接口，Bond qinq 子接口。
创建 vlan 普通三层接口；命令如 interface Vlan20
创建 Eth 接口，命令如 interface eth0-1
创建 Eth 接口的子接口，命令如 interface eth0-1.5
创建 Eth 得 qinq 子接口，命令如 interface eth0-1.5.3
创建 Bond+ID 接口；命令如 interface Bond0
创建 Bond 子接口；命令如 interface Bond0.5
创建 Bond qinq 子接口；命令如 interface Bond0.5.3

【命令模式】 配置模式

【参数说明】

参数	说明
IFNAME	接口名， 如：vlan2~vlan4094 或 eth0-1~eth4-6 (7000), eth1-1 ~ eth1-24 (5000), bond0～bond7
	子接口名，如： eth3-5.10 为接口 eth3-5 创建子接口，tag 值为 10
	qinq 子接口名，如： eth3-5.10.3 为接口 eth3-5.10 创建子接口，外层 tag（s-tag）值为 10，内层 tag(c-tag)为 3

【默认状态】 无

【使用指导】 若接口不存在，创建接口后进入 interface 结点；接口已存在则直接进入 interface 结点。**创建 vlan 三层接口**必须先创建二层 vlan。vlan1 不允许创建三层接口。

子接口的创建目前只支持端口高级路由接口作为父接口，对普通端口的接口和普通 vlan 接口不支持。若端口不在 tag 值所对应的 vlan 中，命令会自动将端口以 tag 模式加入 tag 值所对应的 vlan 中（主控板端口除外）

必须先创建 BONDX 接口，而且往 BONDX 中加入了至少一个接口，才能给 BONDX 创建子接口或者 qinq 子接口。子接口 tag 的取值范围[2, 4095]，其他操作与 eth 口创建的子接口一样。

【配置实例】
```
interface vlan10
interface eth1-5
interface eth0-1.5.3
interface Bond0
interface Bond0.5
interface Bond0.5.3
```

2.2.2 no interface IFNAME

【命令格式】 **no interface IFNAME**

【命令功能】 删除三层接口或各类子接口

【命令模式】 配置模式

【参数说明】

参数	说明
IFNAME	接口名，如：vlan3，eth3-5，eth1-2.3，bond0，bond0.2，

bond0.2.5

【默认状态】

【使用指导】 必须先创建 vlan 接口。若存在子接口，则必须选删除子接口。删除子接口命令会自动将端口从 tag 对应的 vlan 中删除。

【配置实例】 no interface vlan10
no interface eth1-5

2.3 配置三层接口

2.3.1 ip address

【命令格式】 **ip address A.B.C.D/M**

【命令功能】 配置接口 IP address

【命令模式】 interface 配置模式

【参数说明】

参数	说明
A.B.C.D/M	Ip 地址和子网掩码位数

【默认状态】 无

【使用指导】 不能和已有 ip 地址网段相交。

【配置实例】 ip address 10.0.0.1/8

2.3.2 no ip address

【命令格式】 no ip address A.B.C.D/M

【命令功能】 删除接口的 IP 地址

【命令模式】 interface 配置模式

【参数说明】

参数	说明
A.B.C.D/M	为接口配置的 IP 地址，例如：10.0.0.1/8

【默认状态】 无

【使用指导】 无

【配置实例】 no ip address 10.0.0.1/8

2.3.3 ipv6 address

【命令格式】 **ipv6 address A.B.C.D/M**

【命令功能】 配置接口 IPv6 address

【命令模式】 interface 配置模式

【参数说明】

参数	说明
A.B.C.D/M	Ipv6 地址和子网掩码位数

【默认状态】 无

【使用指导】　不能和已有 ipv6 地址网段相交。
【配置实例】　ipv6 address 1111:1111::1/64

2.3.4 no ipv6 address

【命令格式】　no ipv6 address A.B.C.D/M
【命令功能】　删除接口的 IPv6 地址
【命令模式】　interface 配置模式
【参数说明】

参数	说明
A.B.C.D/M	为接口配置的 IPv6 地址，例如：1111:1111::1/64

【默认状态】　无
【使用指导】　无
【配置实例】　no ip address 1111:1111::1/64

2.3.5 shutdown

【命令格式】　shutdown
【命令功能】　关闭该接口，使该接口 down 状态
【命令模式】　interface 配置模式
【参数说明】　无
【默认状态】　无
【使用指导】　实现对内核中接口状态的修改
【配置实例】　shutdown

2.3.6 no shutdown

【命令格式】　no shutdown
【命令功能】　启动该接口，使该接口 up 状态
【命令模式】　interface 配置模式
【参数说明】　无
【默认状态】　无
【使用指导】　实现对内核中接口状态的修改
【配置实例】　no shutdown

2.3.7 advanced-routing

【命令格式】　advanced-routing (enable|disable)
【命令功能】　创建 vlan 高级路由三层接口或端口的高级路由接口
【命令模式】　interface 配置模式

【参数说明】

参数	说明
enable	创建高级路由接口
disable	删除高级路由接口并创建新的普通三层接口

【默认状态】

【使用指导】 必须先创建二层 vlan, 并创建三层接口，或创建端口的三层接口。配置高级路由使能，是将原三层接口删除，并创建新的高级路由接口，因此原接口存在的所有配置都将丢失。

【配置实例】 advanced-routing enable

2.3.8 link-detect

【命令格式】 link-detect

【命令功能】 启动该接口的链路检测功能

【命令模式】 interface 配置模式

【参数说明】 无

【默认状态】 关闭

【使用指导】 当该功能打开后，接口的 UP 状态随着接口物理 up down 状态发生变化，当该功能关闭时，接口的 UP 状态不随接口的物理 up down 状态发生变化。

【配置实例】 link-detect

2.3.9 no link-detect

【命令格式】 no link-detect

【命令功能】 取消该接口的链路检测功能

【命令模式】 interface 配置模式

【参数说明】 无

【默认状态】 关闭

【使用指导】 当该功能打开后，接口的 UP 状态随着接口物理 up down 状态发生变化，当该功能关闭时，接口的 UP 状态不随接口的物理 up down 状态发生变化。

【配置实例】 no link-detect

2.3.10 config qinq-type VALUE

【命令格式】 **config qinq-type VALUE**

【命令功能】 配置接口支持 802.1ad 时的 s-tag 值

【命令模式】 interface 配置模式

【参数说明】

参数	说明
VALUE	Type value ,eg. 0x8100, 0, 10000

【默认状态】 0

【使用指导】　仅支持子接口下配置此命令，不支持父接口和 qinq 接口，要配置之前，先创建此接口，并进入接口结点。仅在从该接口发送多层 tag 的包时，对最外层 tag 起作用。除 0，0x8100 和 0x88a8 以外，最多配置 16 个不同的值，默认配置为 0，配置为 0 时可认为是删除了该配置。

【配置实例】　config qinq-type 0x8888

2.3.11 add bonding interface

【命令格式】　add　bonding　IFNAME

【命令功能】　给 bond 接口添加绑定的接口

【命令模式】　interface 配置模式

【参数说明】

参数	说明
IFNAME	需要往 bond 接口添加的绑定接口

【使用指导】　先创建一个 bond 接口，再添加

【配置实例】
```
interface bond0
add　bonding eth1-10
add　bonding eth1-11
```

2.3.12 delete bonding interface

【命令格式】　delete　bonding　IFNAME

【命令功能】　从 bond 接口删除绑定的接口

【命令模式】　interface 配置模式

【参数说明】

参数	说明
IFNAME	需要从 bond 接口删除的绑定接口

【使用指导】　无

【配置实例】
```
interface bond0
delete　bonding eth1-10
delete　bonding eth1-11
```

2.3.13 set mode

【命令格式】　set mode (balance-rr|active-backup|balance-xor|broadcast|802.3ad
|balance-tlb|balance-alb)

【命令功能】　设置 bond 口报文发送模式

【命令模式】　interface 配置模式

【参数说明】

参数	说明
balance-rr	平衡轮循环。传输数据包顺序是依次传输，直到最后一个传输完毕，此模式提供负载平衡和容错能力。
active-backup	主-备份。只有一个设备处于活动状态，一个宕掉另一个马上由备份转换为主设备。此模式提供了容错能力。
balance-xor	哈希平衡。传输根据原地址布尔值选择传输设备，此模式提供负载平衡和容错能力。
broadcast	广播。将所有数据包传输给所有接口，此模式提供了容错能力。
802.3ad	动态链接聚合。创建共享相同的速度和双工设置的聚合组。
balance-tlb	传出自动负载均衡。
balance-alb	传出及传入皆自动负载均衡。

【默认参数】 balance-rr
【使用指导】 无
【配置实例】 interface bond0
set mode 802.3ad
interface bond1
set mode balance-rr

2.4 显示三层接口信息

2.4.1 **show interface**

【命令格式】 **show interface [IFNAME]**
【命令功能】 显示系统接口信息
【命令模式】 系统模式、配置模式
【参数说明】

参数	说明
IFNAME（可选）	若无参数，则显示系统下所有接口信息，如输入该参数则仅显示该接口的信息

【默认状态】 无
【使用指导】 无
【配置实例】 show interface
show interface vlan10

2.4.2 show bonding BONDX

【命令格式】 show bonding BONDX
【命令功能】 显示 bonding 接口包含了哪些接口
【命令模式】 配置模式
【参数说明】

参数	说明
BONDX	Bonding 接口名，bond0～bond7

【使用指导】 无
【配置实例】 show bonding bond0

3 配置ARP

3.1ARP 功能简介

在局域网中，当主机或其他网络设备有数据要发给另一个主机或设备时，它不仅需要知道目的设备的 IP 地址，还必须知道目的设备的物理地址，因此设备需要一个从 IP 地址到物理地址的映射。ARP 协议就是实现这个从 IP 地址到物理地址转换功能的协议。

一个网络设备需要将报文发送给另一个设备，而不知道对方的 MAC 地址时，便会发送 arp 请求，目的设备收到后发送 arp 回复报文。设备通过解析 arp 回复报文得到目的 MAC 地址，并在自己的 arp 表中添加 IP 地址到 MAC 地址的映射表项，方便后续报文的转发。

ARP 表项分为动态 ARP 表项和静态 ARP 表项：

动态表项由 ARP 协议通过报文自动生成和维护，定期老化，也可以被新的 arp 报文更新和覆盖。静态表项有管理员手动设置，不会老化，也不会被动态表项覆盖。

3.2 配置 ARP

3.2.1 ip static-arp

【命令格式】 ip static-arp PORTNO MAC IP/32 <1-4095> (普通端口，7000/5612i 业务板)
ip static-arp PORTNO MAC IP/32 （7000 主控口）（1.2 不支持保存该配置，且未区分千、万兆小卡或 7000 主控口）
ip static-arp <1-127> MAC IP/32 <1-4095> (for trunk) （1.2 不支持保存该配置）
【命令功能】 配置静态 arp
【命令模式】 配置模式
【参数说明】

参数	说明
PORTNO	端口格式 slot/port 或 slot-port，slot 表示以太网端口所在设备槽号，port 表示以太网端口所在槽位的本地端口号。如：1/1 或 1-1 表示槽 1 上端口 1
<1-127>	trunk Id
MAC	mac 地址
IP	ip 地址和掩码 如 1.1.1.1/32
<1-4094>	vlan ID

【默认状态】 无
【使用指导】 命令创建静态 arp，ip 掩码必须是 32 位
【配置实例】 ip static-arp 1/1 00:11:22:33:44:55 10.0.0.1/32 1

3.2.2 **no ip static-arp**

【命令格式】 no ip static-arp PORTNO MAC IP <1-4094> (普通端口，7000/5612 业务板)
no ip static-arp PORTNO MAC IP （7000/5612 主控板）
no ip static-arp <1-127> MAC IP <1-4095> (for trunk)
【命令功能】 删除静态 arp
【命令模式】 配置模式
【参数说明】

参数	说明
PORTNO	端口格式 slot/port 或 slot-port，slot 表示以太网端口所在设备槽号，port 表示以太网端口所在槽位的本地端口号。如：1/1 或 1-1 表示槽 1 上端口 1
<1-127>	trunk Id
MAC	mac 地址
IP	ip 地址和掩码
<1-4094>	vlan ID

【默认状态】 无
【使用指导】 命令删除静态 arp，ip 掩码必须是 32 位
【配置实例】 no ip static-arp 1/1 00:11:22:33:44:55 10.0.0.1/32 1

3.2.3 **add arp IP MAC base IFNAME**

【命令格式】 add arp IP MAC base IFNAME
【命令功能】 添加删除静态 arp
【命令模式】 配置模式
【参数说明】

参数	说明
IP	设置静态 arp 的 IP 信息
MAC	静态 arp 的 MAC 信息
IFNAME	静态 arp 针对的接口名称

【使用指导】 无
【配置实例】 add arp 192.168.1.1 00:11:E0:DA:C2:78 base eth0-1

3.2.4 **del arp IP MAC base IFNAME**

【命令格式】 del arp IP MAC base IFNAME
【命令功能】 添加删除静态 arp
【命令模式】 配置模式
【参数说明】

参数	说明
IP	设置静态 arp 的 IP 信息
MAC	静态 arp 的 MAC 信息
IFNAME	静态 arp 针对的接口名称

【使用指导】 无
【配置实例】 del arp 192.168.1.1 00:11:E0:DA:C2:78 base eth0-1

3.2.5 **config arp smac-check**

【命令格式】 config arp smac-check (enable|disable)
【命令功能】 检查 arp 的源 mac
【命令模式】 配置模式
【参数说明】

参数	说明
enable	进行 arp 报文二层的源 mac 和 arp 中的发送 mac 检查
disable	不进行 arp 报文二层的源 mac 和 arp 中的发送 mac 检查

【默认状态】 无
【使用指导】 对 arp 进行安全检查
【配置实例】 config arp smac-check enable

3.2.6 clear eth-port arp

【命令格式】 clear eth-port PORTNO arp [static]
【命令功能】 清除端口 ARP 信息
【命令模式】 配置模式
【默认状态】 无
【参数说明】

参数	说明
PORTNO	端口格式 slot/port 或 slot-port，slot 表示以太网端口所在设备槽号，port 表示以太网端口所在槽位的本地端口号。如：1/1 或 1-1 表示槽 1 上端口 1

【默认状态】 无
【使用指导】 清除此端口上的 arp 信息。
【配置实例】 clear eth-port 2/6 arp

3.2.7 clear trunk arp

【命令格式】 clear trunk <1-127> arp [static]
【命令功能】 清除当前 trunk 中的 arp。
【命令模式】 配置模式
【参数说明】

参数	说明
<1-127>	trunk ID

【默认状态】 无
【使用指导】 必须先创建 trunk
【配置实例】 clear trunk 1 arp

3.3 显示 ARP 信息

3.3.1 show arp list

【命令格式】 show arp list
【命令功能】 显示设备缓存中的所有 ARP 表项
【命令模式】 系统模式、配置模式
【使用指导】 ARP 表项内容包括：邻居设备的 IP 地址、邻居设备的 MAC 地址、接口名、状态

【配置实例】 show arp list

3.3.2 show arp by interface

【命令格式】 show arp by interface IFNAME
【命令功能】 按接口名显示 arp 条目
【命令模式】 系统模式、配置模式
【参数说明】

参数	说明
IFNAME	Interface name

【使用指导】 将显示所有通过该接口与本设备发生通信的设备的信息
【配置实例】 show arp by interface eth1-12

3.3.3 show arp by ip

【命令格式】 show arp by ip A.B.C.D
【命令功能】 按 IP 地址显示 ARP 条目
【命令模式】 系统模式、配置模式
【参数说明】

参数	说明
A.B.C.D	IP 地址

【使用指导】 可用来检查某设备是否与本设备发生过通信
【配置实例】 show arp by ip 1.1.1.1

3.3.4 show arp by mac

【命令格式】 show arp by mac XX:XX:XX:XX:XX:XX
【命令功能】 显示设备中 ARP 表项
【命令模式】 系统模式、配置模式
【参数说明】

参数	说明
XX:XX:XX:XX:XX:XX	设备的 MAC 地址

【配置实例】 show arp by mac 00:25:64:c5:e8:3f

3.3.5 show arp by state

【命令格式】 show arp by state (delay | noarp | permanent | probe | reachable | stale)
【命令功能】 按状态显示 arp 条目
【命令模式】 系统模式、配置模式
【参数说明】

参数	说明
delay	若包被发送到相关项处于过期状态的邻居时，该邻居地址被标记为 delay
noarp	标记该邻居不需要任何协议来解决三层到二层的地址映射
permanent	标记该邻居地址被静态配置，永久存在
probe	过度状态，本设备在判断该邻居地址是否可达
reachable	标记该邻居地址是可访问的
stale	标记该邻居地址已过期

【使用指导】 无
【配置实例】 show arp by state reachable

3.3.6 show eth-port arp

【命令格式】 show eth-port PORTNO arp
【命令功能】 显示端口 ARP 信息
【命令模式】 配置模式
【参数说明】

参数	说明

PORTNO	端口格式 slot/port 或 slot-port，slot 表示以太网端口所在设备槽号，port 表示以太网端口所在槽位的本地端口号。如：1/1 或 1-1 表示槽 1 上端口 1

【默认状态】 无
【使用指导】 ARP 信息包括：IP 地址、MAC 地址，槽号端口号,VLAN ID, 端口属性，VIDX、TrunkId，是否为静态 ARP。
【配置实例】 show eth-port 2/6 arp

3.3.7 **show trunk arp**

【命令格式】 show trunk <1-127> arp
【命令功能】 以列表方式显示当前 trunk 中的 arp。
【命令模式】 配置模式
【参数说明】

参数	说明
<1-127>	Trunk ID

【默认状态】 无
【使用指导】 必须先创建 trunk
【配置实例】 show trunk 1 arp

4 配置DHCP server

4.1DHCP server 功能简介

DHCP 即动态主机配置协议，主要解决大规模网络中计算机的 IP 地址分配问题。DHCP 采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等配置信息，实现网络资源的动态配置。

4.2 配置 DHCP server 全局参数

4.2.1 **ip dhcp server enable**

【命令格式】 ip dhcp server enable
【命令功能】 开启 dhcp server。
【命令模式】 配置模式
【参数说明】 无

【默认状态】 无
【使用指导】 无
【配置实例】 ip dhcp server enable

4.2.2 ip dhcp server disable

【命令格式】 ip dhcp server disable
【命令功能】 关闭 dhcp server
【命令模式】 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
【配置实例】 ip dhcp server disable

4.2.3 ip dhcp server domain

【命令格式】 ip dhcp server domain NAME
【命令功能】 配置全局的 domain
【命令模式】 配置模式
【参数说明】

参数	说明
NAME	文本字符串，以字母、下划线开头，允许包含@字符；支持最大域名长度为 20 个字符

【默认状态】 无
【使用指导】 无
【配置实例】ip dhcp server domain autelan

4.2.4 no ip dhcp server domain

【命令格式】 no ip dhcp server domain
【命令功能】 删除全局的 domain 配置
【命令模式】 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
【配置实例】no ip dhcp server domain

4.2.5 ip dhcp server dns

【命令格式】 ip dhcp server dns A.B.C.D [A.B.C.D] [A.B.C.D]
【命令功能】 配置全局的 dns。
【命令模式】 配置模式

【参数说明】

参数	说明
A.B.C.D	域名服务器 IP 地址

【使用指导】 设置 1 到 3 个 dns ip。

【配置实例】 ip dhcp server dns 192.168.1.18

4.2.6 no ip dhcp server dns

【命令格式】 no ip dhcp server dns

【命令功能】 删除全局的 dns 设置

【命令模式】 配置模式

【参数说明】 无

【使用指导】 无

【配置实例】 no ip dhcp server dns

4.2.7 ip dhcp server wins

【命令格式】 ip dhcp server wins A.B.C.D

【命令功能】 配置全局的 wins

【命令模式】 配置模式

【参数说明】

参数	说明
A.B.C.D	WINS 服务器 IP 地址

【使用指导】 无

【配置实例】 ip dhcp server wins 192.168.1.18

4.2.8 no ip dhcp server wins

【命令格式】 no ip dhcp server wins

【命令功能】 删除全局的 wins 配置

【命令模式】 配置模式

【参数说明】 无

【使用指导】 无

【配置实例】 no ip dhcp server wins

4.2.9 ip dhcp server lease-default

【命令格式】 ip dhcp server lease-default

【命令功能】 恢复全局的 lease time 为 default。

【命令模式】 配置模式

【参数说明】 无

【使用指导】 默认值 86400，单位为秒
【配置实例】ip dhcp server lease-default

4.2.10 ip dhcp server lease-time

【命令格式】 ip dhcp server lease-time TIME
【命令功能】配置全局的 lease time。
【命令模式】 配置模式
【参数说明】

参数	说明
TIME	用户租期，范围为 60-31536000，单位：秒

【默认状态】默认值 86400，单位为秒
【使用指导】 无
【配置实例】ip dhcp server lease-time 20000

4.2.11 ip dhcp static

【命令格式】 ip dhcp static A.B.C.D HH:HH:HH:HH:HH:HH IFNAME
【命令功能】 配置指定接口的静态地址绑定信息。
【命令模式】 配置模式
【参数说明】

参数	说明
A.B.C.D	用户 IP 地址
HH:HH:HH:HH:HH:HH	用户 MAC 地址
IFNAME	指定的三层接口

【使用指导】 无
【配置实例】 ip dhcp static 192.168.3.2 00:1E:90:B1:A4:D0 eth.0-1

4.2.12 no ip dhcp static

【命令格式】 no ip dhcp static A.B.C.D HH:HH:HH:HH:HH:HH IFNAME
【命令功能】 删除指定接口的静态地址绑定信息配置
【命令模式】 配置模式
【参数说明】

参数	说明
A.B.C.D	用户 IP 地址
HH:HH:HH:HH:HH:HH	用户 MAC 地址
IFNAME	指定的三层接口

【使用指导】 无
【配置实例】 no ip dhcp static 192.168.3.2 00:1E:90:B1:A4:D0 eth.0-1

4.2.13 ip dhcp reply-mode

【命令格式】ip dhcp reply-mode (unicast|default)
【命令功能】控制 dhcp server offer 回复方式
【命令模式】配置模式
【参数说明】

参数	说明
unicast	强制 offer 单播回复
default	默认方式（广播或单播）方式回复，

【使用指导】 无
【配置实例】ip dhcp reply-mode unicast

4.3 配置 DHCP server 的 IP 地址池

4.3.1 ip pool

【命令格式】 ip pool NAME
【命令功能】 创建 ip 地址池
【命令模式】 配置模式
【参数说明】

参数	说明
NAME	文本字符串，以字母、下划线开头，支持最大地址池名长度为 20 个字符（地址名称合法字符包括：大写字母、小写字母、数字及四种特殊符号 - _ . @）

【使用指导】 使用该命令创建地址池的同时会进入 ip pool 配置模式，可以对地址池进行配置。
【配置实例】ip pool vlan100

4.3.2 no ip pool

【命令格式】 no ip pool NAME
【命令功能】 删除 ip 地址池
【命令模式】 配置模式
【参数说明】

参数	说明
NAME	文本字符串，以字母、下划线开头，支持最大地址池名长度为 20 个字符（地址名称合法字符包括：大写字母、小写字母、数字及四种特殊符号 - _ .

	@）

【使用指导】 无
【配置实例】 no ip pool vlan100

4.3.3 config ip pool

【命令格式】 config ip pool NAME
【命令功能】 ip pool 配置模式
【命令模式】 配置模式
【参数说明】

参数	说明
NAME	需要进行配置的地址池名称

【使用指导】 无
【配置实例】config ip pool vlan100

4.3.4 add range

【命令格式】 add range A.B.C.D A.B.C.D mask A.B.C.D
【命令功能】 增加 ip 地址段。
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
A.B.C.D	地址池起始、结束 IP 地址；地址池掩码，格式形如 255.255.0.0

【使用指导】 注意掩码与接口掩码保持一致
【配置实例】 add range 192.168.4.4 192.168.4.8 mask 255.255.255.0

4.3.5 delete range

【命令格式】 delete range A.B.C.D A.B.C.D mask A.B.C.D
【命令功能】 删除 ip 地址段。
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
A.B.C.D	地址池起始、结束 IP 地址；地址池掩码，格式形如 255.255.0.0

【使用指导】 注意掩码与接口掩码保持一致
【配置实例】 delete range 192.168.4.4 192.168.4.8 mask 255.255.255.0

4.3.6 ip dhcp server dns

【命令格式】 ip dhcp server dns A.B.C.D [A.B.C.D] [A.B.C.D]
【命令功能】 配置当前地址池的 dns。
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
A.B.C.D	域名服务器 IP 地址

【使用指导】 配置 1 到 3 个 dns ip。
【配置实例】 ip dhcp server dns 192.168.1.18

4.3.7 no ip dhcp server dns

【命令格式】 no ip dhcp server dns
【命令功能】 删除当前地址池的 dns 配置
【命令模式】 ip pool 配置模式
【参数说明】 无
【使用指导】 无
【配置实例】 no ip dhcp server dns

4.3.8 ip dhcp server wins

【命令格式】 ip dhcp server wins A.B.C.D
【命令功能】 配置当前地址池的 wins
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
A.B.C.D	WINS 服务器 IP 地址

【使用指导】 无
【配置实例】 ip dhcp server wins 192.168.1.18

4.3.9 no ip dhcp server wins

【命令格式】 no ip dhcp server wins
【命令功能】 删除当前地址池的 wins 配置
【命令模式】 ip pool 配置模式
【参数说明】 无
【使用指导】 无
【配置实例】 no ip dhcp server wins

4.3.10 ip dhcp server lease-default

【命令格式】 ip dhcp server lease-default
【命令功能】 恢复当前地址池的 lease time 为 default
【命令模式】 ip pool 配置模式
【参数说明】 无
【使用指导】 默认值为 86400，单位为秒
【配置实例】ip dhcp server lease-default

4.3.11 ip dhcp server lease-time

【命令格式】 ip dhcp server lease-time TIME
【命令功能】 配置当前地址池的 lease time。
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
TIME	用户最大租期，范围为 60-31536000，单位：秒

【默认状态】默认值为 86400，单位为秒
【使用指导】 无
【配置实例】ip dhcp server lease-time 20000

4.3.12 ip dhcp server domain

【命令格式】 ip dhcp server domain NAME
【命令功能】 配置当前地址池的 domain name
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
NAME	文本字符串，以字母、下划线开头，允许包含@字符；支持最大域名长度为 20 个字符

【使用指导】 无
【配置实例】ip dhcp server domain autelan

4.3.13 no ip dhcp server domain

【命令格式】 no ip dhcp server domain
【命令功能】 删除当前地址池的 domain name 配置
【命令模式】 ip pool 配置模式
【参数说明】 无
【使用指导】 无
【配置实例】 no ip dhcp server domain

4.3.14 ip dhcp server option43

【命令格式】 ip dhcp server option43 (HEX| A.B.C.D)
【命令功能】 配置当前地址池的 option43
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
HEX	16 进制字符串，
A.B.C.D	Ipv4 地址，最多可配置 16 个

【使用指导】 无
【配置实例】ip dhcp server option43 1108c007a812c0a80715
option43 后接 16 进制字符串，11 代表 type，08 表示有 2 个 ip，04 代表 1 个 ip，依次类推，后边是 ip 地址的 16 进制表示。
ip dhcp server option43 192.168.4.2

4.3.15 no ip dhcp server option43

【命令格式】 no ip dhcp server option43 [HEX| A.B.C.D]
【命令功能】 取消当前地址池的 option43 配置
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
HEX	16 进制字符串，
A.B.C.D	Ipv4 地址，最多可配置 16 个

【使用指导】 无
【配置实例】no ip dhcp server option43 1108c007a812c0a80715
option43 后接 16 进制字符串，11 代表 type，08 表示有 2 个 ip，04 代表 1 个 ip，依次类推，后边是 ip 地址的 16 进制表示。
no ip dhcp server option43 192.168.4.2

4.3.16ip dhcp server option138

【命令格式】 ip dhcp server option138 A.B.C.D
【命令功能】 配置当前地址池的 option138
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
A.B.C.D	Ipv4 地址，最多可配置 16 个

【使用指导】 无
【配置实例】ip dhcp server option138 192.168.4.2

4.3.17 no ip dhcp server option138

【命令格式】 no ip dhcp server option138 [A.B.C.D]
【命令功能】 取消当前地址池的 option138 配置
【命令模式】 ip pool 配置模式
【参数说明】

参数	说明
A.B.C.D	Ipv4 地址

【使用指导】 无
【配置实例】 no ip dhcp server option138

4.4 配置三层接口绑定 IP 地址池

4.4.1 ip pool

【命令格式】 ip pool NAME
【命令功能】 绑定地址池。
【命令模式】 interface 配置模式
【参数说明】

参数	说明
NAME	已创建的地址池名称

【使用指导】 需要进入具体的接口下进行绑定操作
【配置实例】ip pool autelan

4.4.2 no ip pool

【命令格式】 no ip pool NAME
【命令功能】 取消绑定地址池。
【命令模式】 interface 配置模式
【参数说明】

参数	说明
NAME	已创建的地址池名称

【使用指导】 需要进入具体得接口下，取消绑定时需要将 dhcp 服务关闭。
【配置实例】no ip pool autelan

4.5 显示 DHCP server 配置信息

4.5.1 show ip dhcp

【命令格式】show ip dhcp
【命令功能】 查看全局的 dhcp 配置。
【命令模式】 配置模式
【参数说明】 无
【使用指导】 无
【配置实例】show ip dhcp

4.5.2 show ip pool

【命令格式】show ip pool
【命令功能】 查看地址池配置。
【命令模式】、配置模式、ip pool 配置模式
【参数说明】 无
【使用指导】配置模式下，查看系统中所有地址池的配置。
ip pool 配置模式下，查看当前地址池配置；
【配置实例】show ip pool

4.5.3 show ip dhcp static

【命令格式】show ip dhcp static
【命令功能】查看静态绑定用户信息。
【命令模式】配置模式
【参数说明】 无
【使用指导】无
【配置实例】show ip dhcp static

4.5.4 show dhcp-lease

【命令格式】show dhcp-lease
show dhcp-lease by A.B.C.D
show dhcp-lease ip_range A.B.C.D A.B.C.D
show dhcp-lease by subnet A.B.C.D/M
show dhcp-lease by MAC
【命令功能】查看全部/给定 IP/网段/MAC 的 lease 信息
【命令模式】配置模式
【参数说明】

参数	说明
A.B.C.D	IP 地址

A.B.C.D	起始 IP 地址、结束 IP 地址
A.B.C.D/M	起始 IP 地址, M 表示掩码长度
MAC	MAC 地址

【使用指导】

【配置实例】show dhcp-lease

show dhcp-lease by 192.158.7.123

show dhcp-lease ip_range 192.168.4.5 192.168.4.15

show dhcp-lease by subnet 192.168.7.4/24

show dhcp-lease by 00:1E:90:B1:A4:D0

5 配置DHCP Relay

5.1DHCP Relay 功能简介

由于动态获取 IP 采用的是广播方式发送请求报文，因此 DHCP 只适用于客户端和服务器在同一子网的情况。为了解决每个网段都需要配置 dhcp 服务器，引入了 Dhcp Relay 功能。Dhcp Relay 将客户端的 dhcp 请求发送给 dhcp 服务器，并将服务器的 dhcp 回复发送给客户端，实现了 dhcp 客户端与不同网段的服务器通信，这样，多个网段的 dhcp 客户端就可以使用同一个 dhcp 服务器，既节约了成本，又方便集中管理。

5.2配置 DHCP Relay

5.2.1 ip dhcp relay enable|disable

【命令格式】 ip dhcp relay (enable|disable)

【命令功能】 配置 dhcp relay 服务的状态

【命令模式】 配置模式

【参数说明】

参数	说明
enable	开启 DHCP Relay 服务
disable	关闭 DHCP Relay 服务

【使用指导】 无

【配置实例】 ip dhcp relay enable

5.2.2 ip relay IFNAME

【命令格式】 ip relay IFNAME A.B.C.D

【命令功能】 配置 dhcp relay 转发接口名和地址

【命令模式】 interface 配置模式

【参数说明】

参数	说明
IFNAME	转发目的 server 接口名
A.B.C.D	目的 server ip 地址

【使用指导】 无

【配置实例】 ip relay eth1-9 192.168.4.8 或 ip relay vlan2 192.168.4.8

5.2.3 no ip relay IFNAME

【命令格式】 no ip relay IFNAME A.B.C.D

【命令功能】 取消 dhcp relay 转发接口名和地址配置

【命令模式】 interface 配置模式

【参数说明】

参数	说明
IFNAME	目的 server 网络接口名
A.B.C.D	目的 server ip 地址

【使用指导】

【配置实例】no ip relay eth1-9 192.168.4.8 或 no ip relay vlan2 192.168.4.8

5.3 显示 DHCP Relay 配置

5.3.1 show ip dhcp relay

【命令格式】show ip dhcp relay

【命令功能】 查看 dhcp relay 配置

【命令模式】 配置模式

【参数说明】 无

【使用指导】 无

【配置实例】show ip dhcp relay

6 配置DHCP Snooping

6.1 DHCP Snooping 功能简介

DHCP Snooping 工作于 DHCP 客户端与 DHCP 服务器或者 DHCP 中继之间，监听 DHCP 报文，建立客户端 IP 和 MAC 的对应表项，并保证客户端从合法的服务器获取 IP 地址。

DHCP Snooping 功能可以运用到 LAN 口，也可以运用到 WAN 口。本模块配置将 DHCP Snooping 根据作用接口的不同，分为两种模式：LAN 模式和 WAN 模式，并按照这两种模式分别定义配置命令。LAN 模式和 WAN 模式可以同时启用，也可以分别启用。

6.2 配置 LAN 模式全局 DHCP Snooping

6.2.1 config dhcp-snooping lan

【命令格式】 config dhcp-snooping lan (enable|disable)
【命令功能】 使能设备 DHCP Snooping 功能。
【命令模式】 配置模式
【参数说明】

参数	说明
enable/disable	使能/禁用 DHCP Snooping

【使用指导】

config dhcp-snooping lan enable 命令用来开启交换机 LAN 口 DHCP Snooping 功能。

config dhcp-snooping lan disable 命令用来关闭 LAN 口 DHCP Snooping 功能。在 DHCP Snooping 功能关闭后，所有端口都可转发 DHCP 服务器的响应报文，并且不记录 DHCP 客户端的 IP 地址和 MAC 地址。

缺省情况下，交换机的 DHCP Snooping 功能处于关闭状态。

需要注意的是：

- 开启设备的 DHCP Snooping 功能之前，需要先关闭其 DHCP 中继功能。
- 开启设备的 DHCP Snooping 功能之前，需要开启全局 ACL 服务(config acl service enable）。
- 开启 DHCP Snooping 功能后，不支持与之连接的客户端使用 BOOTP 方式动态获取 IP 地址。

【配置实例】config dhcp-snooping enable

6.2.2 config dhcp-snooping information

【命令格式】 config dhcp-snooping information (enable|disable)
【命令功能】 开启/关闭 DHCP Snooping 支持 Option 82 功能
【命令模式】 配置模式
【参数说明】

参数	说明
enable/disable	开启/关闭 DHCP Snooping 支持 Option 82 功能

【默认状态】

缺省情况下，DHCP Snooping 支持 Option 82 功能处于关闭状态。

【使用指导】

config dhcp-snooping information enable 命令用来开启 DHCP Snooping 支持 Option 82 功能。

config dhcp-snooping information disable 命令用来关闭 DHCP Snooping 支持 Option 82 功能。

需要注意的是，只有支持 DHCP Snooping 的设备，开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】config dhcp-snooping information enable

6.2.3 config dhcp-snooping information format

【命令格式】 config dhcp-snooping information format (hex|ascii)
【命令功能】 配置非用户自定义的 DHCP Snooping Option 82 子选项的存储格式
【命令模式】 配置模式
【参数说明】

参数	说明
hex	指定 Option 82 存储格式是 HEX，即十六进制数串格式
ascii	指定 Option 82 存储格式是 ASCII（美国信息交换标准码）格式。

【默认状态】

缺省情况下，DHCP Snooping 支持 Option 82 的存储格式为 HEX。

【使用指导】

config dhcp-snooping information format 命令用来配置非用户自定义的 DHCP Snooping Option 82 子选项的存储格式为 HEX 或 ASCII 格式。

需要注意的是，只有支持 DHCP Snooping 的设备，开启 DHCP Snooping 功能后，才支持此项配置。

config dhcp-snooping information format 命令只对交换机默认填加的 Option 82 内容生效。如果用户通过命令配置了 Circuit ID 或 Remote ID 的内容，则相应子选项的填充格式为 ASCII 格式，不再受 config dhcp-snooping information format 命令配置的约束。

【配置实例】config dhcp-snooping information format hex

6.2.4 config dhcp-snooping information packet-format

【命令格式】 config dhcp-snooping information packet-format (extended|standard)
【命令功能】 配置 Option 82 字段的填充格式为标准格式或扩展格式
【命令模式】 配置模式
【参数说明】

参数	说明
extended	配置 Option 82 字段的填充格式为扩展格式

standard	配置 Option 82 字段的填充格式为标准格式

【默认状态】

缺省情况下，Option 82 字段的填充格式为扩展格式。

【使用指导】

config dhcp-snooping information packet-format 命令用来配置 Option 82 字段的填充格式为标准格式或扩展格式。

需要注意的是，只有支持 DHCP Snooping 的设备，开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】config dhcp-snooping information packet-format extended

6.2.5 config dhcp-snooping information remote-id

【命令格式】 config dhcp-snooping information remote-id (sysmac|sysname|string STRING)

【命令功能】 配置 Option 82 的 Remote ID 内容

【命令模式】 配置模式

【参数说明】

参数	说明
sysmac	配置 Option 82 的 Remote ID 内容为设备的桥 MAC 地址。
sysname	配置 Option 82 的 Remote ID 内容为设备的系统名。
string STRING	配置 Option 82 的 Remote ID 内容用户自定义配置的 Remote ID 子选项的内容。 STRING：用户自定义配置的 Remote ID 子选项的内容，格式为 ASCII 字符串，取值范围为 1～63 个字符。

【默认状态】

缺省情况下，Option 82 中 Remote ID 内容为接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的桥 MAC 地址。

【使用指导】

config dhcp-snooping information remote-id 命令用来配置 Option 82 的 Remote ID 内容。

需要注意的是，只有支持 DHCP Snooping 的设备，开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】config dhcp-snooping information remote-id sysname

6.2.6 dhcp-snooping static-binding add ip-address

【命令格式】 dhcp-snooping static-binding add ip-address A.B.C.D mac MAC vlan <1-4094>

eth-port PORTNO

【命令功能】 增加源 IP 地址、源 MAC 地址与端口之间的静态绑定关系

【命令模式】 配置模式

【参数说明】

参数	说明
A.B.C.D	IP 地址。
MAC	mac 地址
<1-4094>	VLAN ID，有效值为 1-4094
PORTNO	属于前面配置 vlan 的端口

【使用指导】 只有支持 DHCP Snooping 的设备，开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】 dhcp-snooping static-binding add ip-address 192.168.1.1 mac 00:1F:64:12:33:44 vlan 2 eth-port 1/2

6.2.7 dhcp-snooping static-binding delete ip-address

【命令格式】 dhcp-snooping static-binding delete ip-address A.B.C.D mac MAC vlan <1-4094> eth-port PORTNO

【命令功能】 删除源 IP 地址、源 MAC 地址与端口之间的静态绑定关系

【命令模式】 配置模式

【参数说明】

参数	说明
A.B.C.D	IP 地址。
MAC	mac 地址
<1-4094>	VLAN ID，有效值为 1-4094
PORTNO	属于前面配置 vlan 的端口

【使用指导】只有支持 DHCP Snooping 的设备，开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】 dhcp-snooping static-binding delete ip-address 192.168.1.1 mac 00:1F:64:12:33:44 vlan 2 eth-port 1/2

6.3配置 LAN 模式 VLAN 节点下的 DHCP Snooping

6.3.1 config dhcp-snooping

【命令格式】 config dhcp-snooping (enable|disable)

【命令功能】 在特定 vlan 上使能 DHCP Snooping 功能。

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
enable|disable	使能或禁用 vlan 的 DHCP Snooping 功能。

【默认状态】缺省情况下，vlan 的 DHCP Snooping 功能处于关闭状态。

【使用指导】 先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置。开启 vlan 上的 DHCP Snooping 功能，必须保证全局的 DHCP Snooping 功能已经开启。

【配置实例】 config dhcp-snooping enable

6.3.2 config dhcp-snooping PORTNO mode

【命令格式】 config dhcp-snooping PORTNO (trust|trust-nobind|notrust)

【命令功能】 配置端口为 DHCP Snooping 信任端口/信任不绑定端口/不信任端口

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
PORTNO	指定要配置的端口号。端口格式如下：1/1 或 1-1，2/1，2-6，分别表示槽位号和端口号。
trust| trust-nobind| notrust	必选参数三选一，配置端口为 DHCP Snooping 信任端口/信任不绑定端口/不信任端口。

【默认状态】缺省情况下，开启 vlan 的 DHCP Snooping 功能后，vlan 的所有端口均为 DHCP Snooping 不信任端口。

【使用指导】

先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置；在开启 vlan 的 DHCP Snooping 功能之后，才可以进行端口的 DHCP Snooping 功能配置；对端口配置 DHCP Snooping 相关功能时，该端口必须保证其为当前 VLAN 配置模式下 vlan 的成员。

- config dhcp-snooping PORTNO trust 命令用来配置端口为 DHCP Snooping 信任端口。
- config dhcp-snooping PORTNO trust-nobind 命令用来配置端口为 DHCP Snooping 信任但不绑定端口。
- config dhcp-snooping PORTNO notrust 命令用来恢复端口为 DHCP Snooping 不信任端口。

需要注意的是：开启 DHCP Snooping 功能后，为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口,且设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。

【配置实例】

config dhcp-snooping 1/2 trust

6.3.3 config dhcp-snooping information strategy PORTNO ploicy

【命令格式】

config dhcp-snooping information strategy PORTNO (drop|keep|replace)

【命令功能】 配置指定端口接收的 DHCP 客户端发送的包含 Option 82 选项请求报文配置处理策略

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
PORTNO	指定要配置的端口号。端口格式如下：1/1 或 1-1，2/1，2-6，分别表示槽位号和端口号。
drop	如果报文中带有 Option 82 选项，则 DHCP Snooping 丢弃该报文。
keep	如果报文中带有 Option 82 选项，则 DHCP Snooping 保持该报文中的 Option 82 选项不变并进行转发。
replace	如果报文中带有 Option 82 选项，DHCP Snooping 按照配置的填充内容填充 Option 82 选项，并替换报文中原有的 Option 82 选项进行转发。

【默认状态】 缺省情况下，当开启 DHCP Snooping 支持 Option 82 功能后，DHCP Snooping 设备对 DHCP 客户端发送的带有 Option 82 选项的请求报文的处理策略为 replace。

【使用指导】

先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置；在开启 vlan 的 DHCP Snooping 功能之后，才可以进行端口的 DHCP Snooping 功能配置；对端口配置 DHCP Snooping 相关功能时，该端口必须保证其为当前 VLAN 配置模式下 vlan 的成员。

在 vlan 下执行 config dhcp-snooping information strategy 命令用来对指定端口接收的 DHCP 客户端发送的包含 Option 82 选项请求报文配置处理策略。只有支持 DHCP Snooping 的设备开启 DHCP Snooping 功能以及 vlan 开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】 config dhcp-snooping information strategy 1/1 drop

6.3.4 config dhcp-snooping information circuit-id PORTNO content

【命令格式】

config dhcp-snooping information circuit-id PORTNO (default|string STRING)

【命令功能】 配置端口上 Option 82 的 Circuit ID 字段内容

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
PORTNO	指定要配置的端口号。端口格式如下：1/1 或 1-1，

	2/1，2-6，分别表示槽位号和端口号。
default	配置端口上 Option 82 的 Circuit ID 字段内容为接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引。
string STRING	配置端口上 Option 82 的 Circuit ID 内容为用户自定义配置的 Circuit ID 子选项的内容。 STRING：用户自定义配置的 Circuit ID 字段的内容，格式为 ASCII 字符串，取值范围为 3～63 个字符。

【默认状态】

缺省情况下，Option 82 的 Circuit ID 内容为接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口索引。

【使用指导】

先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置；在开启 vlan 的 DHCP Snooping 功能之后，才可以进行端口的 DHCP Snooping 功能配置；对端口配置 DHCP Snooping 相关功能时，该端口必须保证其为当前 VLAN 配置模式下 vlan 的成员。

在 vlan 下执行 config dhcp-snooping information circuit-id 命令用来对指定端口配置 Option 82 的 Circuit ID 字段内容。

注意：

只有支持 DHCP Snooping 的设备开启 DHCP Snooping 功能以及 vlan 开启 DHCP Snooping 功能后，才支持此项配置。

【配置实例】

```
config dhcp-snooping information circuit-id 1/1 default
```

6.3.5 config dhcp-snooping information remote-id PORTNO content

【命令格式】

```
config dhcp-snooping information remote-id PORTNO (default|string STRING)
```

【命令功能】 配置端口上 Option 82 的 Remote ID 字段内容

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
PORTNO	指定要配置的端口号。端口格式如下：1/1 或 1-1，2/1，2-6，分别表示槽位号和端口号。
default	配置端口上 Option 82 的 Remote ID 字段内容为接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的桥 MAC 地址。
string STRING	配置端口上 Option 82 的 Remote ID 内容为用户自定义配置的 Remote ID 子选项的内容。 STRING：用户自定义配置的 Remote ID 字段的内容，格式为 ASCII 字符串，取值范围为 3～63 个字符。

【默认状态】

缺省情况下，Option 82 的 Remote ID 内容为接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的桥 MAC 地址。

【使用指导】

先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置；在开启 vlan 的 DHCP Snooping 功能之后，才可以进行端口的 DHCP Snooping 功能配置；对端口配置 DHCP Snooping 相关功能时，该端口必须保证其为当前 VLAN 配置模式下 vlan 的成员。

在 vlan 下执行 config dhcp-snooping information remote-id 命令用来对指定端口配置 Option 82 的 Remote ID 字段内容。

注意：

- 只有支持 DHCP Snooping 的设备开启 DHCP Snooping 功能以及 vlan 开启 DHCP Snooping 功能后，才支持此项配置。
- 如果在配置模式下已经配置了 Remote ID 的内容，则对于指定端口上的 DHCP 报文，优先使用该端口的 Remote ID 非默认的配置内容进行处理。

【配置实例】

```
config dhcp-snooping information remote-id 1/1 default
```

6.4 配置 WAN 模式全局 DHCP Snooping

6.4.1 config dhcp-snooping wan

【命令格式】 config dhcp-snooping wan (enable|disable)

【命令功能】 全局开启/关闭设备 WAN 口 DHCP Snooping 功能。

【命令模式】 配置模式

【参数说明】

参数	说明
enable/disable	使能/禁用 DHCP Snooping

【使用指导】

config dhcp-snooping wan enable 命令用来开启交换机 WAN 口 DHCP Snooping 功能。config dhcp-snooping wan disable 命令用来关闭 WAN 口 DHCP Snooping 功能。在 DHCP Snooping 功能关闭后，所有 WAN 口不监听 DHCP 报文，并且不记录 DHCP 客户端的 IP 地址和 MAC 地址。

缺省情况下，交换机 WAN 口的 DHCP Snooping 功能处于关闭状态。

【配置实例】config dhcp-snooping wan enable

6.4.2 config dhcp-snooping IFNAME

【命令格式】 config dhcp-snooping IFNAME (enable|disable)

【命令功能】开启/关闭设备上特定 WAN 口 DHCP Snooping 功能。
【命令模式】 配置模式
【参数说明】

参数	说明
IFNAME	WAN 口的接口名
enable/disable	使能/禁用 DHCP Snooping

【使用指导】
开启特定 WAN 口 DHCP Snooping 功能之前，需要全局打开 WAN 口的 DHCP Snooping 功能。
【配置实例】config dhcp-snooping eth0-1 enable

6.5配置 WAN 模式接口节点下的 DHCP Snooping

6.5.1 **config dhcp-snooping enable|disable**

【命令格式】 config dhcp-snooping (enable|disable)
【命令功能】使能设备上特定 WAN 口 DHCP Snooping 功能，作用同 7.4.1。
【命令模式】 interface 配置模式
【参数说明】

参数	说明
enable/disable	使能/禁用 DHCP Snooping

【使用指导】开启特定 WAN 口 DHCP Snooping 功能之前，需要全局打开 WAN 口的 DHCP Snooping 功能。
【配置实例】config dhcp-snooping enable

6.6 显示 DHCP Snooping 配置信息

6.6.1 **show dhcp-snooping**

【命令格式】 show dhcp-snooping
【命令功能】 显示通过 DHCP Snooping 记录的用户 IP 地址和 MAC 地址的对应关系
【命令模式】 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 无
show dhcp-snooping 命令用来显示通过 DHCP Snooping 记录的用户 IP 地址和 MAC 地址的对应关系。必须保证全局的 DHCP Snooping 功能已经开启。
【配置实例】 show dhcp-snooping

6.6.2 show dhcp-snooping trust

【命令格式】 show dhcp-snooping trust
【命令功能】 显示 DHCP Snooping 开启状态及信任端口信息
【命令模式】 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】show dhcp-snooping trust 命令用来显示 DHCP Snooping 开启状态及信任端口信息。必须保证全局的 DHCP Snooping 功能已经开启。
【配置实例】 show dhcp-snooping trust

6.6.3 show dhcp-snooping static-binding

【命令格式】 show dhcp-snooping static-binding
【命令功能】 显示通过静态添加的 IP 地址和 MAC 地址的对应关系
【命令模式】 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 show dhcp-snooping static-binding 命令用来显示通过静态添加的 IP 地址和 MAC 地址的对应关系。必须保证全局的 DHCP Snooping 功能已经开启。
【配置实例】 show dhcp-snooping static-binding

6.6.4 show dhcp-snooping static-binding vlan

【命令格式】 show dhcp-snooping static-binding vlan <1-4094>
【命令功能】 显示特定 VLAN 中通过静态添加的 IP 地址和 MAC 地址的对应关系
【命令模式】 配置模式
【参数说明】

参数	说明
<1-4094>	VLAN ID，有效值为 1-4094

【默认状态】
【使用指导】
show dhcp-snooping static-binding vlan <1-4094> 命令用来显示特定 VLAN 中通过静态添加的 IP 地址和 MAC 地址的对应关系。必须保证全局的 DHCP Snooping 功能已经开启。
【配置实例】 show dhcp-snooping static-binding vlan 2

6.6.5 show dhcp-snooping static-binding eth-port PORTNO

【命令格式】 show dhcp-snooping static-binding eth-port PORTNO
【命令功能】 显示特定端口上通过静态添加的 IP 地址和 MAC 地址的对应关系
【命令模式】 配置模式

【参数说明】

参数	说明
PORTNO	指定要配置的端口号。端口格式如下：1/1 或 1-1，2/1，2-6，分别表示槽位号和端口号。

【默认状态】 无

【使用指导】

show dhcp-snooping static-binding eth-port PORTNO 命令用来显示特定端口上通过静态添加的 IP 地址和 MAC 地址的对应关系。必须保证全局的 DHCP Snooping 功能已经开启。

【配置实例】 show dhcp-snooping static-binding eth-port 1/2

7 配置IGMP Snooping

7.1 IGMP Snooping 功能简介

IGMP Snooping 是互联网组播管理协议窥探的简称，用于二层网络管理和控制组播组。IGMP Snooping 通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。

IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，具有以下优点：

减少了二层网络中的广播报文，节约了网络带宽；

增强了组播信息的安全性；

为实现对每台主机的单独计费带来了方便。

在设备上与 IGMP Snooping 相关的端口分两种：路由器端口，指设备上朝向三层组播设备一侧的端口；成员端口，设备上朝向组播组成员一侧的端口。这里的端口均包括静态和动态端口。

7.2 配置全局 IGMP Snooping

7.2.1 **config igmp-snooping**

【命令格式】 config igmp-snooping (enable|disable)

【命令功能】 使能设备 IGMP Snooping 功能。

【命令模式】 配置模式

【参数说明】

参数	说明
enable/disable	使能/禁用 IGMP Snooping

【使用指导】 设备启动之后，需要对其进行全局的使能配置。没有全局地使能，设备将不支持 IGMP Snooping 功能；

【配置实例】 config igmp-snooping enable

7.2.2 **config igmp-snooping timeout**

【命令格式】

configigmp-snooping(vlan-lifetime|group-lifetime|robust|query-interval|response-interval) TIMEOUT

【命令功能】 配置 IGMP snooping 协议时间参数

【命令模式】 配置模式

【参数说明】

参数	说明
vlan-lifetime	vlan-lifetime 指定 vlan 中有组播组形成后，组播组宿主 vlan 的生存时间。
group-lifetime	group-lifetime 指定组播组的生存时间。
robust	robust 参数为可靠性常量，默认值为 2。
query-interval	query-interval 指定宿主 vlan 向其所有使能 IGMP Snooping 的端口成员发送 IGMP general query 报文的周期时间间隔。
response-interval	response-interval 指定所有使能 IGMP Snooping 的多播组成员响应 qurey 报文的允许时间间隔。

【默认状态】 vlan lifetime 默认值：42000
Group lifetime 默认值：21000
Robust variable 默认值：2
Query interval 默认值：5000
response-interval 默认值：500

【有效值域】 vlan lifetime 有效值：[10000 - 100000]
Group lifetime 有效值：[1000 - 50000]
Robust variable 有效值：[1 - 100]
Query interval 有效值：[1000 - 10000]
response-interval 有效值：[100 - 1000]
单位：毫秒

【使用指导】 IGMP Snooping 运行需要的定时参数，用户输入合法范围内的值，则进行配置，若超出范围，将不改变当前配置继续运行。另外，当没有全局地使能 IGMP Snooping 时，将不能对参数进行配置。

【配置实例】 config igmp-snooping vlan-lifetime 20000
config igmp-snooping query-interval 1500

7.3配置 vlan 节点下的 IGMP Snooping

7.3.1 **config igmp-snooping enable|disable**

【命令格式】 config igmp-snooping (enable|disable)

【命令功能】 在特定 vlan 上使能 IGMP Snooping 功能。

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
(enable|disable)	使能或禁用 vlan 的 IGMP Snooping 功能。vlan 中可以形成一个或多个组播组。

【默认状态】

【使用指导】 先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置。开启 vlan 上的 IGMP Snooping 功能，必须保证全局的 IGMP Snooping 功能已经开启。

【配置实例】
```
config vlan 2
config igmp-snooping enable
```

7.3.2 config igmp-snooping PORTNO enable|disable

【命令格式】 config igmp-snooping PORTNO (enable|disable)

【命令功能】 使能/禁止 vlan 成员端口的 IGMP Snooping 功能

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
PORTNO	指定要添加到 IGMP Snooping 协议运算的端口号。端口格式如下：1/1 或 1-1，2/1，2-6，分别表示槽位号和端口号，其中槽位号有效值为 1～4，端口号的范围为 1～6
enable|disable	必选参数二选一，指定 vlan 端口成员 enable 或 disable 组播 IGMP Snooping 功能

【默认状态】

【使用指导】 先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置；在开启 vlan 的 IGMP Snooping 功能之后，才可以进行端口的 IGMP Snooping 功能配置；端口使能/禁用 IGMP snooping 功能时，该端口必须保证其为当前 VLAN 配置模式下 vlan 的成员。

【配置实例】
```
config vlan 2
config igmp-snooping enable
config igmp-snooping 1/2 enable
```

7.3.3 add|delete igmp-snooping route-port PORTNO

【命令格式】 (add|delete) igmp-snooping route-port PORTNO

【命令功能】 将某端口设置为组播组路由端口，用于完成向网络中组播路由器发送本地及 subnet 中的组播信息

【命令模式】 VLAN 配置模式

【参数说明】

参数	说明
add|delete	必选参数二选一，指定端口使能或禁止其成为路由端口
PORTNO	指定组播路由器端口的端口号。端口格式如下：1/1 或 1-1，2/1，2-6，分别表示槽位号和端口号，其中槽位号有效值为 1～4，端口号的范围为 1～6

【默认状态】

【使用指导】 先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后进行该命令行配置。要配置为路由端口的 vlan 端口成员必须已经使能了该端口上 IGMP Snooping 功能。在一个 vlan 内，最多只能有一个路由端口。

【配置实例】
```
config vlan 2
config igmp-snooping 1/2 enable
add igmp-snooping route-port 1/2
```

7.4 显示 IGMP Snooping 配置

7.4.1 show igmp-snooping time-interval

【命令格式】 show igmp-snooping time-interval

【命令功能】 显示 IGMP Snooping 当前相关时间参数

【命令模式】 配置模式

【参数说明】 无

【默认状态】 无

【使用指导】 显示当前配置的时间参数。在没有全局地使能 IGMP Snooping 时，将不能显示协议的时间参数。

【配置实例】 show igmp-snooping time-interval

7.4.2 show igmp-snooping vlan-count

【命令格式】 show igmp-snooping vlan-count

【命令功能】 显示设备中当前使能 IGMP snooping 功能的 vlan 数目

【命令模式】 配置模式

【参数说明】 无

【默认状态】 无

【使用指导】 无

【配置实例】 show igmp-snooping vlan-count

7.4.3 show igmp-snooping vlan-list

【命令格式】 show igmp-snooping vlan-list

【命令功能】 显示设备中当前使能 IGMP snooping 功能的 vlan 的详细信息，

包括 vlanID 和支持 IGMP snooping 功能的端口列表

【命令模式】 配置模式

【参数说明】 无

【默认状态】 无

【使用指导】 无

【配置实例】 show igmp-snooping vlan-list

7.4.4 show igmp-snooping group-count

【命令格式】 show igmp-snooping group-count

【命令功能】 显示设备当前形成的组播组数目

【命令模式】 配置模式

【参数说明】 无

【使用指导】 无

【配置实例】 show igmp-snooping group-count

7.4.5 show igmp-snooping group-list vlan

【命令格式】 show igmp-snooping group-list vlan <1-4094>

【命令功能】 显示设备当前在特定 vlan 下形成的组播组列表

【命令模式】 配置模式

【参数说明】

参数	说明
<1-4094>	指定 vlanid 对应的 VLAN，设备支持 4K 个 VLAN。其中，1 为缺省 VLAN

【使用指导】 无

【配置实例】 show igmp-snooping group-list vlan 1

7.4.6 show igmp-snooping route-port vlan

【命令格式】 show igmp-snooping route-port vlan <1-4094>

【命令功能】 显示设备在特定 vlan 下用户配置的路由端口和实际使用的路由端口(包括没有配置路由端口时由 PIM 协议的 hello 报文得到的路由端口)

【命令模式】 配置模式

【参数说明】

参数	说明
<1-4094>	指定 vlanid 对应的 VLAN，设备支持 4K 个 VLAN。其中，1 为缺省 VLAN

【使用指导】 无

【配置实例】 show igmp-snooping route-port vlan 1

7.4.7 show multicast-group count

【命令格式】 show multicast-group count
【命令功能】 显示设备当前形成的组播组数目
【命令模式】 VLAN 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 显示 VLAN 中，当前存在的组播组的数量。
【配置实例】 show multicast-group count

7.4.8 show multicast-group list

【命令格式】 show multicast-group list
【命令功能】 显示当前 VLAN 中存在的组播组的基本信息，包括 vidx、vlan id、组播组 IP 地址，以及组成员端口列表
【命令模式】 VLAN 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后执行本命令行，可以显示当前 vlan 中形成的组播组的信息。

【配置实例】 config vlan 2
show multicast-group list

7.4.9 show multicast-group route-port

【命令格式】 show multicast-group route-port
【命令功能】 显示当前 VLAN 中用户配置的路由端口列表和实际使用的路由端口（包括由 PIM 协议的 hello 报文得到的路由端口）
【命令模式】 VLAN 配置模式
【参数说明】 无
【默认状态】 无
【使用指导】 先调用 config vlan <2-4094> <vlanname>.进入 vlan 配置模式,然后执行本命令，显示当前 vlan 中，用户配置的路由端口。用于指定的路由端口，必须保证其上的 IGMP Snooping 功能已经开启。
【配置实例】 config vlan 2
show multicast-group route-port

8 配置ACL

8.1ACL 功能简介

ACL 即访问控制列表，通过配置对报文的匹配规则和处理操作来实现包过滤的功能，对报文匹配的规则包括报文的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、协议类型。ACL 配置时注意以下说明：

说明①：标准和扩展的规则 acl 索引的关系是.：当配置一条扩展 ext rule 时，由于硬件特殊要求，须将相邻的空间也一并占据。举例：ext rule 5，那么在硬件空间里，索引为 5，5+500 的空间都被占据，所以如果要设置标准规则的时候，标准索引 517 的规则由于没有内存存放，使得无法下发。目前版本建议大家索引取值 1-500。

说明②：如果有规则覆盖的流，取索引号小的 acl。即匹配最详细的规则可能被范围较大的规则覆盖，那么如果一条流同时匹配了两条规则，取索引号小的 acl。建议规则比较详细的 acl 设成索引号比较小的规则。

说明③：在添加 acl rule 到 ingress group 和 egress group 是有区别的。Ingress group 对于除 egress-qos 之外的的任何设定的 acl rule 都可以添加。但是 egress group 只能添加动作为 permit，deny 或 egress-qos 的 acl rule。

说明④：对于入口的基于端口的 acl 服务，需要分别进行使能设置。

说明⑤：实现 acl 功能，必须要使能全局 acl 服务。命令见[config acl service]。

特别说明⑥：只有 action 为 permit 和 redirect 的才允许 policer。

8.2 配置 ACL

8.2.1 config acl service

【命令格式】 config acl service (enable|disable)

【命令功能】 开启或者关闭全局 ACL 服务

【命令模式】 配置模式

【默认状态】 disable

【参数说明】

参数	说明
enable	开启 ACL 功能
dsable	关闭 ACL 功能

【使用指导】 使用该命令能够使能全局 ACL 服务。

【配置实例】 config acl service enable

8.2.2 acl ip (permit|deny| trap)

【命令格式】 acl (standard|extended) <1-1000>(permit|deny| trap) ip dip (A.B.C.D/M|any) sip (A.B.C.D/M|any) [policer] [<1-255>]

【命令功能】 配置基于 ip 报文的 acl 规则，动作为 permit，deny，trap-to-cpu 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的取值范围
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
A.B.C.D/M	IP 地址和掩码
any	任意 IP 地址
policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。standard 时，acl 取值范围为 1-1000，extended 时 acl 取值范围为 1-500。 下同。

【配置实例】 acl standard 5 deny ip dip 10.1.1.5/32 sip any

8.2.3 acl ip redirect

【命令格式】 acl (standard|extended) <1-1000> redirect PORTNO ip dip (A.B.C.D/M|any)sip(A.B.C.D/M|any) [policer <1-255>]

【命令功能】 配置基于 ip 报文的 acl 规则，动作为 redirect

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的取值范围
redirect	匹配规则后的策略处理，重定向
PORTNO	重定向目的槽号和端口号，槽号(1－4)，端口号(1－6)
A.B.C.D/M	IP 地址和掩码
any	任意 IP 地址

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。在使用 redirect 命令时，如果目的端口不在同一 vlan，请先使用 config vlan egress-filter disable，否则报文会被丢弃。

【配置实例】 **acl standard 5 redirect 2/3 ip dip 10.1.1.5/32 sip any**

8.2.4 acl (tcp | udp) (permit | deny | trap)

【命令格式】 acl (standard|extended) <1-1000> (permit | deny | trap) (tcp | udp) dip (A.B.C.D/M|any) dst-port (<0-65535>|any) sip (A.B.C.D/M|any)src-port (<0-65535>|any) [policer] [<1-255>]

【命令功能】 配置基于 tcp，udp 报文的 acl 规则，动作为 permit，deny，trap-to-cpu 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的取值范围
Tcp	匹配 TCP 报文
Udp	匹配 udp 报文
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
A.B.C.D/M	IP 地址和掩码
<0-65535>	源，目的端口号
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl standard 5 deny tcp dip 10.1.1.5/32 dst-port 21 sip any src-port 1000

8.2.5 acl (tcp | udp) redirect

【命令格式】 acl (standard|extended) <1-1000> redirect PORTNO (tcp | udp) dip (A.B.C.D/M|any) dst-port (<0-65535>|any) sip(A.B.C.D/M|any) src-port (<0-65535>|any) [policer] [<1-255>]

【命令功能】 配置基于 tcp，udp 报文的 acl 规则，动作为 redirect

【命令模式】 配置模式

【参数说明】

参数	说明

<1-1000>	acl 的取值范围
Tcp	匹配 TCP 报文
Udp	匹配 udp 报文
redirect	匹配规则后的策略处理，重定向
PORTNO	重定向目的槽号和端口号，槽号(1－4)，端口号(1－6)
A.B.C.D/M	IP 地址和掩码
<0-65535>	源，目的端口号

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl standard 5 redirect 2/3 tcp dip 10.1.1.5/32 Dst-port 21 sip any src-port 1000

8.2.6 acl icmp (permit | deny | trap)

【命令格式】 acl (standard|extended) <1-1000> (permit | deny | trap) icmp dip (A.B.C.D/M|any) sip (A.B.C.D/M|any) type (<0-255>|any) code(<0-255>|any) [policer] [<1-255>]

【命令功能】 配置基于 icmp 报文的 acl 规则，动作为 permit，deny，trap-to-cpu 任何一种。

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的取值范围
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
<0-255>	Icmp type，code
A.B.C.D/M	IP 地址和掩码
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 无

【配置实例】 acl standard 5 deny icmp dip 10.2.2.2/32 sip any type 3 code 6

8.2.7 **acl icmp redirect**

【命令格式】 acl (standard|extended) <1-1000> redirect PORTNO icmp dip (A.B.C.D/M|any) sip (A.B.C.D/M|any) type (<0-255>|any) code (<0-255>|any)

【命令功能】 配置基于 icmp 报文的 acl 规则，动作为 redirect

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的取值范围
redirect	匹配规则后的策略处理，重定向
PORTNO	重定向目的槽号和端口号，槽号(1－4)，端口号(1－6)
<0-255>	Icmp type
<0-255>	Icmp code
A.B.C.D/M	IP 地址和掩码
<0-65535>	源，目的端口号

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl standard 5 redirect 2/3 icmp dip 10.2.2.2/32 sip any type 3 code

8.2.8 **acl arp (permit | deny | trap)**

【命令格式】 acl extended <1-500> (permit | deny | trap) arp smac (H:H:H:H:H:H) vid <1-4095> sourceport PORTNO [policer] [<1-255>]

【命令功能】 配置基于 arp 报文的 acl 规则，动作为 permit，deny，trap-to-cpu 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的 extended 取值范围
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
H:H:H:H:H:H	源 MAC 的地址
<1-4095>	vlan 取值

PORTNO	接收包的端口 slot/port，或 slot-port
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl extended 5 deny arp smac 11:22:33:44:55:66 vid 30 sourceport 1/3

8.2.9 acl arp(redirect| mirror)

【命令格式】 acl extended <1-1000> (redirect)
PORTNO arp smac (H:H:H:H:H:H) vid <1-4095> sourceport PORTNO

【命令功能】 配置基于 arp 报文的 acl 规则，动作为 redirect ，mirror-to-analyzer 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
mirror	匹配规则后的策略处理，镜像到分析端口

redirect	匹配规则后的策略处理，重定向
PORTNO	重定向或镜像目的槽号和端口号，槽号(1－4)，端口号(1－6)
H:H:H:H:H:H	源 MAC 的地址
<1-4095>	vlan 取值
PORTNO	接收包的端口 slot/port 或 slot-port

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1

【配置实例】 acl extended 5 redirect 2/3 arp smac 11:22:33:44:55:66 vid 30 sourceport 2/3

8.2.10 acl Ethernet (permit | deny | trap)

【命令格式】 acl extended <1-500> (permit | deny | trap) Ethernet
dmac (H:H:H:H:H:H |any) smac (H:H:H:H:H:H |any)
[policer] [<1-255>]

【命令功能】 配置基于非 ip 报文的 acl 规则，动作为 permit，deny，trap-to-cpu

任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
H:H:H:H:H:H	源，目的 MAC 的地址
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl extended 5 deny ethernet dmac 11：22：33：22：11：22 smac 55：44：33：33：33：22

8.2.11 **acl Ethernet redirect**

【命令格式】 acl extended <1-500> redirect PORTNO ethernet dmac (H:H:H:H:H:H |any) smac (H:H:H:H:H:H |any)

【命令功能】 配置基于非 ip 报文的 acl 规则，动作为 redirect

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
redirect	匹配规则后的策略处理，重定向
PORTNO	重定向目的槽号和端口号，槽号(1－4)，端口号(1－6)
H:H:H:H:H:H	源，目的 MAC 的地址

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl extended 7 redirect 1/3 ethernet dmac 11:22:33:44:55:66 smac 66:55:44:33:22:11

8.2.12 acl extended (permit | deny| trap) (tcp|udp)

【命令格式】 acl extended <1-500> (permit | deny | trap) (tcp | udp) dip (A.B.C.D/M|any) dst-port (<0-65535>|any) sip (A.B.C.D/M|any) src-port (<0-65535>|any) dmac (H:H:H:H:H:H |any) smac (H:H:H:H:H:H |any) vid (<1-4095> |any) sourceport (PORTNO |any) [policer] [<1-255>]

【命令功能】 配置基于 tcp 或 udp 报文的 acl 扩展规则，动作为 permit，deny，trap-to-cpu 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
Tcp	匹配 tcp 报文
Udp	匹配 udp 报文
A.B.C.D/M	目的，源 IP 地址
<0-65535>	目的，源端口号
H:H:H:H:H:H	目的，源 MAC 地址
<1-4095>	Vlan id
PORTNO	包近来的端口号
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置扩展 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1

【配置实例】 acl extended 32 deny tcp dip 10.2.2.2/32 dst-port 21 sip 10.2.2.5/32 src-port any dmac 00:19:25:00:00:4f smac any vid 1 sourceport 1/3

8.2.13 acl extended redirect (tcp|udp)

【命令格式】 acl extended <1-500> redirect PORTNO(tcp|udp) dip (A.B.C.D/M|any) dst-port (<0-65535>|any) sip (A.B.C.D/M|any) src-port (<0-65535>|any) dmac (H:H:H:H:H:H |any) smac (H:H:H:H:H:H |any) vid

【命令功能】 配置基于 tcp 或 udp 报文的 acl 扩展规则，动作为 redirect

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
redirect	匹配规则后的策略处理，重定向
PORTNO	重定向目的槽号和端口号，槽号(1－4)，端口号(1－6)sourceport 后面的端口号是包进来的端口号
Tcp	匹配 tcp 报文
Udp	匹配 udp 报文
A.B.C.D/M	目的，源 IP 地址
<0-65535>	目的，源端口号
H:H:H:H:H:H	目的，源 MAC 地址
<1-4095>	Vlan id

【使用指导】 使用该命令能够配置扩展 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1

【配置实例】 acl extended 43 redirect 1/3 tcp dip 10.2.2.2/32 dst-port 21 sip 10.2.2.5/32 src-port any dmac 00:19:25:00:00:4f smac any vid 1 sourceport 1/3

8.2.14 acl ethertype (permit | deny | trap)

【命令格式】 acl extended <1-500> (permit | deny | trap) ethertype (<0-65534>|any) dmac (H:H:H:H:H:H |any) smac (H:H:H:H:H:H |any) [policer] [<1-255>]

【命令功能】 配置基于特定的 ethertype 报文的 acl 规则，动作为 permit、deny、trap-to-cpu 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
<0-65534>|any	Ethertype 取值范围
H:H:H:H:H:H	源，目的 MAC 的地址
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl extended 5 deny ethertype 123 dmac 11:22:33:44:55:66 smac 66:55:44:33:22:11

8.2.15 acl ethertype redirect

【命令格式】 acl extended <1-500> redirect PORTNO ethertype (<0-65534>|any) dmac (H:H:H:H:H:H |any) smac (H:H:H:H:H:H |any)

【命令功能】 配置基于特定的 ethertype 报文的 acl 规则，动作为 redirect

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
redirect	匹配规则后的策略处理，重定向
<0-65534>|any	Ethertype 取值范围
PORTNO	重定向目的槽号和端口号，槽号(1－4)，端口号(1－6)
H:H:H:H:H:H	源，目的 MAC 的地址

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl extended 89 redirect 1/3 ethernet dmac 11:22:33:44:55:66 smac 66:55:44:33:22:11

8.2.16 acl ipv6 tcp|udp (permit | deny | trap)

【命令格式】 acl extended <1-500> (permit|deny) (tcp|udp)
dipv6 (IPV6|any) dst-port (<0-65535>|any) sipv6 (IPV6|any)
src-port (<0-65535>|any)

【命令功能】 配置基于特定的 ipv6 next-header 报文的 acl 规则，动作为 permit，deny，trap-to-cpu 任何一种

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围

permit	匹配规则后的策略处理，permit 为允许
deny	匹配规则后的策略处理，deny 为拒绝
trap	匹配规则后的策略处理，转发到 CPU
Tcp|udp	Next-header 取值
IPV6 | any	目的 ipv6 地址
<0-65535>|any	目的端口号
IPV6 | any	源 ipv6 地址
<0-65535>|any	源端口号
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段，不支持动作为 trap 的流。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。

【配置实例】 acl extended 99 deny tcp dipv6 any dst-port any sipv6 any src-port any

8.2.17 **delete acl**

【命令格式】 delete acl INDEX

【命令功能】 删除已配置的 ACL 规则

【命令模式】 配置模式

【参数说明】

参数	说明
INDEX	acl 的取值范围。标准规则范围为 1-1000，扩展规则范围为 1-500

【使用指导】 使用该命令能够删除已配置的 ACL 规则。需要注意的是，删除此 acl 规则前提是，该规则尚未加到 acl group 中，或者已加到该 acl group 中并下发到 vlan 或者是端口中。否则，需删除相应的动作，即 acl rule 与 group，vlan，port 无任何牵连的时候才可以删除。此 acl group 包括 ingress ， egress 两种 group。

【配置实例】 delete acl 5

8.2.18 **create acl-group**

【命令格式】 create (ingress | egress) acl-group <1-1023>
【命令功能】 创建入口或出口的 acl group
【命令模式】 配置模式
【参数说明】

参数	说明
ingress	创建 ingress acl group
egress	创建 egress acl group
<1-1023>	Acl group 取值范围

【使用指导】 使用该命令能够创建(ingress/egress) acl-group.两个 group 索引可以相同。
【配置实例】 create ingress acl-group 4

8.2.19 **config acl-group**

【命令格式】 config (ingress | egress) acl-group <1-1023>
【命令功能】 配置入口或者出口的 acl group
【命令模式】 配置模式
【参数说明】

参数	说明
ingress	配置 ingress acl group
egress	配置 egress acl group
<1-1023>	Ingress 或者 egressAcl group 取值范围

【使用指导】 使用该命令，进行配置入口或者出口的 aclgroup 模式，此 group 必须要存在，且并未下发到端口或者 vlan 上。在绑定到 port 或 vlan 上之后，就不能进行 config 操作了。
【配置实例】 config ingress acl-group 4

8.2.20 **add/delete acl**

【命令格式】 (add|delete) acl <1-1000>
【命令功能】 向 acl group 添加/删除 acl rule
【命令模式】 acl-group 配置模式
【参数说明】

参数	说明
Add	添加已配置的 acl rule
Delete	删除已配置的 acl rule
<1-1000>	要添加/删除 acl rule ID

【使用指导】　使用该命令，可在 group 配置模式下进行添加删除已配置 acl rule 的操作。注意是已经在配置模式下存在的 acl rule，另外一点就是不能在两个 group 中添加同一条 acl rule。目前还未做到共享。

【配置实例】　add acl 5

8.2.21 add/delete acl-range

【命令格式】　(add|delete)acl-range <1-1000> <1-1000>

【命令功能】　批量添加 acl rule 到 group 中

【命令模式】　acl-group 配置模式

【参数说明】

参数	说明
Add	添加已配置的 acl rule
Delete	删除已配置的 acl rule
<1-1000>	起始 acl rule 的范围。
<1-1000>	终止 acl rule 的范围。

【使用指导】　使用该命令，可在 group 配置模式下进行添加删除已配置 acl rule 的操作。注意是已经在配置模式下存在的 acl rule，另外一点就是不能在两个 group 中添加同一条 acl rule。目前还未做到共享。

【配置实例】　add acl-range 1 5

8.2.22 acl (enable|disable)

【命令格式】　(ingress | egress)　acl (enable|disable)

【命令功能】　使能端口上的 ACL 服务，或者是使能该 vlan 中所包含所有端口的 acl 服务。有入口和出口之分。

【命令模式】　端口配置模式、VLAN 配置模式

【参数说明】

参数	说明
ingress	ingress acl 服务
egress	egress acl 服务
Enable	使能端口/vlan 的 acl 服务
Disable	关闭端口/vlan 的 acl 服务

【使用指导】　在绑定 acl group 到端口或者 vlan 上时，必须要先使能端口或 vlan 的 acl 服务。有入口和出口之分。

【配置实例】　ingress　acl　enable

8.2.23 acl-range standard ip

【命令格式】 acl-range standard <1-1000> <1-1000> ip-range destination A.B.C.D A.B.C.D source A.B.C.D A.B.C.D [policer <1-255>]

acl-range standard <1-1000> <1-1000> ip-range destination A.B.C.D A.B.C.D source A.B.C.D A.B.C.D [policer-range <1-255><1-255>]

acl-range standard <1-1000> <1-1000> ip-range destination any source A.B.C.D A.B.C.D [policer <1-255>]

acl-range standard <1-1000> <1-1000> ip-range destination any source A.B.C.D A.B.C.D [policer-range <1-255> <1-255>]

acl-range standard <1-1000> <1-1000> ip-range destination A.B.C.D A.B.C.D source any [policer <1-255>]

acl-range standard <1-1000> <1-1000> ip-range destination A.B.C.D A.B.C.D source any policer-range <1-255> <1-255>

【命令功能】 批量配置基于 ip 报文的 acl 规则。

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的 ID，范围为 1-1000，当两个相邻参数都为**<1-1000>**时，前一个为 acl 起始 ID，后一个为终止 ID
A.B.C.D	IP 地址，当两个相邻参数都为 **A.B.C.D** 时，前一个为起始地址，后一个为终止地址
Policer/ policer-range	允许流量监管
<1-255>	流量监管的 policer id，范围为 1-255，当两个相邻参数都为 **<1-255>**时，前一个为 policer 起始 ID，后一个为终止 ID

【使用指导】 使用该命令能够配置 ACL 规则。Policer 为可选字段。选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1。IP 地址范围内包含的 IP 地址个数需和 acl 范围内包含的 acl 数目一致。

8.2.24 acl ingress-qos

【命令格式】 acl extended <1-500> ingress-qos <1-127> sub-qos-markers (enable|disable) source-up (<0-7>|none) source-dscp (<0-63>|none) [policer] [<1-255>]

【命令功能】 配置基于 acl 的 QOS 入口初始化，基于源 up，源 dscp，如果这两

位设置为 none，则代表不关注，不修改相应的 up，或者 dscp。Qos-marker 如果为 disable 时，表示入口引擎之后的其他 markers 无法修改 qos 属性

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
Ingress-qos	匹配报文的 up 和 dscp，进行入口 qos 初始化。
1-127	匹配入口报文的 up 或者 dscp，up 和 dscp 修改为索引为 1-127 的 qos profile 的索引值
<0-7>	入口 vlan tagged 的 up 取取值范围
None	对入口 vlantagged 的 up 和 ip 头的 dscp 不做修改，保留原值
<0-63>	Ip 头的 dscp 取值范围
Enable	允许后面的 markeres 覆盖 qos 的值
Disable	不允许后面的 markers 覆盖已配置的 qos 值
Policer	允许流量监管
<1-255>	流量监管的 policer id 范围

【使用指导】 使用该命令能够配置基于 ACL 规则的入口 QOS 初始化。如果端口的 qos marker 位设置为 disable，则基于 ACL 的 QOS 初始化不能成功。另外一种情况是，ACL 执行顺序为从小到大，（不包括规则相同的报文）如果索引号小的 ACL 的 sub-qos-markers 设定为 disable，则其余索引号大的 ACL 的 ingress-qos 修改 up，dscp 的动作不能实现。Policer 为可选字段，选了此字段，必须设置后面参数，即 policer ID。如果不设，则 policer ID 默认为 -1

【配置实例】 acl extended 5 ingress-qos 5 sub-qos-markers enable source-up none source-dscp 50

8.2.25 acl egress–qos

【命令格式】 acl extended <1-500> egress-qos egress-up <0-7> egress-dscp <0-63> source-up (<0-7>|none) source-dscp (<0-63>|none)

【命令功能】 配置基于 acl 的 QOS 出口重新初始化，基于源 up，源 dscp。如果这两位设置为 none，则代表不关注，不修改相应的 up，或者 dscp，则相应的 egress up 和 egress dscp 设置为任何位都不起作用

【命令模式】 配置模式

【参数说明】

参数	说明
<1-500>	acl 的取值范围
egress-qos	匹配出口报文的 up 和 dscp，再次改变报文的 up 或 dscp
<0-7>	Up 取值范围
None	对入口 vlantagged 的 up 和 ip 头的 dscp 不做修改，保留原值
<0-63>	dscp 取值范围

【使用指导】 使用该命令能够配置基于 ACL 规则的出口 QOS 初始化

【配置实例】 acl extended 5 egress-qos egress-up 4 egress-dscp 34 source-up none source-dscp 50

8.2.26 append acl

【命令格式】 append acl INDEX ingress-qos <1-127>

【命令功能】 将存在的流分类分配 qos 属性，改变 up，dscp

【命令模式】 配置模式

【参数说明】

参数	说明
INDEX	1-512
1-127	支持 127 个 qos profile

【使用指导】 对符合 acl 规则的流进行 qos 操作。

【配置实例】 append acl 1 ingress-qos 2

8.2.27 delete append

【命令格式】 delete append <1-512>

【命令功能】 删除 acl 规则

【命令模式】 配置模式

【参数说明】

参数	说明
<1-512>	INDEX

【使用指导】

【配置实例】 delete append 2

8.2.28 bind/unbind acl-group

【命令格式】 (bind|unbind)(ingress | egress) acl-group <1-1023>

【命令功能】 绑定/解除绑定 acl group 到端口或者 vlan 上

【命令模式】 端口配置模式、VLAN 配置模式

【参数说明】

参数	说明
ingress	ingress acl group
egress	egress acl group
Bind	绑定 acl group 到端口或者 vlan 上
Unbind	解除绑定
<1-1023>	Group 取值范围

【使用指导】 在绑定 acl group 到端口或者 vlan 上时，必须要先使能端口或 vlan 的 acl 服务，且该 group 已配置。有入口和出口之分。

【配置实例】 bind ingress acl-group 4

8.3 显示 ACL

8.3.1 show acl service

【命令格式】 show acl service

【命令功能】 显示全局 ACL 服务

【命令模式】 配置模式

【参数说明】 无

【使用指导】 显示全局 ACL 服务状态

【配置实例】 show acl service

8.3.2 show acl list

【命令格式】 show acl (list | <1-1000>)

【命令功能】 显示已配置的 ACL 规则

【命令模式】 配置模式

【参数说明】

参数	说明
<1-1000>	acl 的取值范围。
list	全部已配置 acl

【使用指导】 使用该命令能够显示已配置的 ACL 规则。使用索引号可精确显示某条 acl rule，使用 list 可显示全部已配置的 acl rule。

【配置实例】 show acl 3

8.3.3 show acl

【命令格式】 show (ingress | egress) acl

【命令功能】　显示端口或者 vlan 上入口或出口的 acl rule 的信息
【命令模式】　端口配置模式、VLAN 配置模式
【参数说明】　无
【使用指导】　显示端口或 vlan 绑定的 acl group ID，group 中所包含的 acl rule 索引，以及 acl rule 个数。有入口出口之分。
【配置实例】　show　ingress　acl

8.3.4 **show acl-group**

【命令格式】　show　(ingress | egress)　acl-group [<1-1023>]
【命令功能】　显示入口或出口的 acl group 信息
【命令模式】　配置模式
【参数说明】

参数	说明
1-1023	Ingress/egress acl group 取值范围

【使用指导】　显示 ingress/egress acl group 信息。加索引号可精确显示某一个 acl group 信息
【配置实例】　show　ingress　acl-group

9 配置Firewall和NAT

9.1 Firewall 和 NAT 功能简介

本章主要介绍了 firewall（filter）、snat、dnat 和 input 四种规则的使用，各类规则作用分别为：
Firewall：对经过本设备的数据包进行过滤（报文源目的地址都不是本设备）；
Snat：进行报文源地址转换；
Dnat：进行报文目的地址转换；
Input：对发往本地的数据包进行过滤（报文目的地址是本设备）。
Index 表示规则的顺序号，从 1 开始计数。
由于规则的内容和选项太多，无法指定一种命令格式能够添加整条规则。所以，可以通过添加（add）命令添加一条默认规则，然后通过指定的索引号（index）来修改（modify）这条规则，以满足您的需求。也就是说，一条规则对应一个 add 命令和若干 modify 命令。
在 add、del、change、modify 规则前，需要停止 firewall 服务（service disable）。

9.2配置 Firewall 和 NAT

9.2.1 **config firewall**

【命令格式】　config firewall
【命令功能】　进入 firewall 配置节点（config-firewall）,在 config-firewall 节点下

可以配置 firewall、snat、dnat 和 input 规则，以及开启/关闭 firewall 服务。

【命令模式】 配置模式

【参数说明】 无

【默认状态】 无

【使用指导】 无

【配置实例】 config firewall

9.2.2 add (firewall|snat|input) desc

【命令格式】 add (firewall|snat|input) desc DESC [INDEX]

【命令功能】 添加一条默认的 firewall 规则

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(firewall|snat|input)	指定添加何种规则
DESC	规则描述
INDEX	规则索引，即规则在链中的顺序

【默认状态】

【使用指导】 添加一条默认的 firewall/snat/input 规则。INDEX 从 1 开始，如果不指定，则将规则添加到末尾。添加后，您可以通过 modify 命令修改它，以满足您的需求。

【配置实例】 add firewall desc aaa

9.2.3 add dnat desc DESC nat-ip

【命令格式】 add dnat desc DESC nat-ip single A.B.C.D [INDEX]
add dnat desc DESC nat-ip mask A.B.C.D/X.X.X.X [INDEX]
add dnat desc DESC nat-ip range A.B.C.D-A.B.C.D [INDEX]

【命令功能】 添加一条默认的 dnat 规则，并指定 DNAT 的 IP 地址或 IP 范围

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
DESC	规则描述
A.B.C.D	DNAT 的 IP 地址
A.B.C.D/X.X.X.X	IP 地址/掩码格式指定的 DNAT 的 IP 范围
A.B.C.D-A.B.C.D	DNAT 的 IP 范围
INDEX	规则索引，即规则在链中的顺序

【默认状态】

【使用指导】 添加一条默认的 dnat 规则，并指定 DNAT 的 IP 地址或范围。INDEX 从 1 开始，如果不指定，则将规则添加到末尾。添加后，您可以通过 modify 命令修改它，以满足您的需求。

【配置实例】 add dnat desc ccc nat-ip single 192.168.10.200 2

add dnat desc ccc nat-ip mask 192.168.10.200/255.255.255.0 2
add dnat desc ccc nat-ip range 192.168.10.200-192.168.10.210

9.2.4 del (firewall|snat|dnat|input)

【命令格式】 del (firewall|snat|dnat|input) INDEX
【命令功能】 按指定的索引号删除规则
【命令模式】 firewall 配置模式
【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定删除何种规则
INDEX	指定要删除规则的索引号

【默认状态】
【使用指导】 按指定的索引号删除规则。删除后，后面的规则前移。
【配置实例】 del snat 2

9.2.5 change (firewall|snat|dnat|input) INDEX index

【命令格式】 change (firewall|snat|dnat|input) INDEX index [NEWINDEX]
【命令功能】 调整规则的顺序，将位于 INDEX 的规则移动到 NEWINDEX 处。
【命令模式】 firewall 配置模式
【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定要调整何种规则
INDEX	指定要移动的规则的索引号
NEWINDEX	指定要移动的规则的新索引号

【默认状态】 无
【使用指导】 调整规则的顺序，将位于 INDEX 的规则移动到 NEWINDEX 处。如果不指定 NEWINDEX，将移动到末尾。
【配置实例】 change firewall 3 index 2

9.2.6 modify (firewall|snat|dnat|input) INDEX desc

【命令格式】 modify (firewall|snat|dnat|input) INDEX desc DESC
【命令功能】 按指定的索引号设置 firewall|snat|dnat|input 规则描述。
【命令模式】 firewall 配置模式
【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定要设置何种规则
INDEX	指定要设置规则的索引号
DESC	规则描述

【默认状态】

【使用指导】 按指定的索引号设置 firewall|snat|dnat|input 规则描述。

【配置实例】 modify firewall 1 desc aaa

9.2.7 modify (firewall|snat|dnat|input) INDEX valid

【命令格式】 modify (firewall|snat|dnat|input) INDEX valid (enable|disable)

【命令功能】 设置指定索引号的规则是否有效。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定要设置何种规则
INDEX	指定要设置规则的索引号
(enable|disable)	enable-有效；disable-无效

【默认状态】 无

【使用指导】 设置指定索引号的规则是否有效。

【配置实例】 modify firewall 1 valid enable

9.2.8 modify firewall INDEX (in-if|out-if)

【命令格式】 modify firewall INDEX (in-if|out-if) (any|INTERFACE)

【命令功能】 按指定的索引号设置 firewall 规则匹配的输入输出接口。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
INDEX	指定要设置规则的索引号
(in-if|out-if)	in-if:输入接口；out-if:输出接口
(any|INTERFACE)	any:任意接口；INTERFACE:指定的接口名

【默认状态】 无

【使用指导】 按指定的索引号设置 firewall 规则匹配的输入输出接口。

【配置实例】 modify firewall 1 in-if eth1-9

9.2.9 modify (dnat|input) INDEX in-if

【命令格式】 modify (dnat|input) INDEX in-if (any|INTERFACE)
【命令功能】 按指定的索引号设置 dnat|input 规则匹配的输入接口。
【命令模式】 firewall 配置模式
【参数说明】

参数	说明
(dnat|input)	指定修改哪种规则
INDEX	指定要设置规则的索引号
(any|INTERFACE)	any:任意接口; INTERFACE:指定的接口名

【默认状态】
【使用指导】 按指定的索引号设置 dnat 规则匹配的输入接口。
【配置实例】 modify dnat 1 in-if any

9.2.10 modify snat INDEX out-if

【命令格式】 modify snat INDEX out-if (any|INTERFACE)
【命令功能】 按指定的索引号设置 snat 规则匹配的输出接口。
【命令模式】 firewall 配置模式
【参数说明】

参数	说明
INDEX	指定要设置规则的索引号
(any|INTERFACE)	any:任意接口; INTERFACE:指定的接口名

【默认状态】
【使用指导】 按指定的索引号设置 snat 规则匹配的输出接口。
【配置实例】 modify snat 1 out-if eth-1-10

9.2.11 modify (firewall|snat|dnat|input) INDEX (src-ip|dst-ip)

【命令格式】 modify (firewall|snat|dnat|input) INDEX (src-ip|dst-ip) any
modify (firewall|snat|dnat|input) INDEX (src-ip|dst-ip) single A.B.C.D
modify (firewall|snat|dnat|input) INDEX (src-ip|dst-ip) mask A.B.C.D/X.X.X.X
modify (firewall|snat|dnat|input) INDEX (src-ip|dst-ip) range A.B.C.D-A.B.C.D
【命令功能】 按指定的索引号设置 firewall|snat|dnat|input 规则匹配的源 IP|目的 IP。
【命令模式】 firewall 配置模式
【参数说明】

参数	说明

(firewall|snat|dnat|input)	指定要设置何种规则
INDEX	指定要设置规则的索引号
(src-ip|dst-ip)	指定要匹配的是源 IP 还是目的 IP。 src-ip:源 IP；dst-ip:目的 IP
A.B.C.D	匹配的 IP 地址
A.B.C.D/X.X.X.X	匹配的 IP 地址/掩码
A.B.C.D-A.B.C.D	匹配的 IP 范围

【默认状态】

【使用指导】 按指定的索引号设置 firewall|snat|dnat|input 规则匹配的源 IP|目的 IP 为任意 IP。

【配置实例】 modify snat 1 src-ip any

modify firewall 2 dst-ip single 100.200.10.20

modify firewall 2 dst-ip mask 100.200.10.20/255.255.0.0

modify firewall 2 dst-ip range 100.200.10.20-100.200.10.50

9.2.12 **modify (firewall|snat|dnat|input) INDEX protocol**

【命令格式】 modify (firewall|snat|dnat|input) INDEX protocol (any|tcp|udp|tcp-and-udp|icmp)

【命令功能】 按指定的索引号设置 firewall|snat|dnat|input 规则匹配的协议。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定要设置何种规则
INDEX	指定要设置规则的索引号
any	任意
tcp	tcp 协议
udp	udp 协议
tcp-and-udp	tcp 和 udp 协议
icmp	icmp 协议

【默认状态】

【使用指导】 按指定的索引号设置 firewall|snat|dnat|input 规则匹配的协议。

【配置实例】 modify firewall 1 protocol udp

9.2.13 **modify (firewall|snat|dnat|input) INDEX (src-port|dst-port)**

【命令格式】 modify (firewall|snat|dnat|input) INDEX (src-port|dst-port) any

modify (firewall|snat|dnat|input) INDEX (src-port|dst-port) single <0-65535>

modify (firewall|snat|dnat|input) INDEX (src-port|dst-port) range PORTRANGE

【命令功能】 按指定的索引号设置 firewall|snat|dnat|input 规则匹配的源|目的端口号。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定要设置何种规则
INDEX	指定要设置规则的索引号
(src-port|dst-port)	指定要匹配的是源端口号还是目的端口号。 src-port:源端口号； dst-port:目的端口号
any	任意的端口号
<0-65535>	指定的端口号
PORTRANGE	指定的端口号范围，以符号“:”连接两个端口号。

【默认状态】

【使用指导】 按指定的索引号设置 firewall|snat|dnat|input 规则匹配的源|目的端口号。设置端口号，需要先将协议设置成 tcp、udp 或者 tcp-and-udp。

【配置实例】
```
modify snat 1 dst-port any
modify snat 1 dst-port single 100
modify snat 1 dst-port range 100:200
```

9.2.14 modify (firewall|input) INDEX state

【命令格式】 modify (firewall|input) INDEX state (new|established|related|invalid) (enable|disable)

【命令功能】 按指定的索引号设置 firewall|input 规则匹配的状态。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
firewall|input	指定修改规则的种类
INDEX	指定要设置规则的索引号
new	NEW 状态
established	ESTABLISHED 状态
related	RELATED 状态
invalid	INVALID 状态
enable	匹配指定的状态
disable	不匹配指定的状态

【默认状态】

【使用指导】 按指定的索引号设置 firewall|input 规则匹配的状态。

【配置实例】
```
modify firewall 1 established enable
```

9.2.15 **modify (firewall|input) INDEX filter-string**

【命令格式】 modify (firewall|input) INDEX filter-string [STRING]

【命令功能】 按指定的索引号设置 firewall|input 规则的过滤字符串。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
firewall|input	指定修改规则的种类
INDEX	指定要设置规则的索引号
[STRING]	过滤字符串，不指定，则为空。

【默认状态】

【使用指导】 按指定的索引号设置 firewall|input 规则的过滤字符串。

【配置实例】 modify firewall 1 filter-string hello

9.2.16 **modify (firewall|input) INDEX act**

【命令格式】 modify (firewall|input) INDEX act (accept|drop|reject)

【命令功能】 按指定的索引号设置 firewall|input 规则匹配后的行为为(accept|drop|reject)。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
firewall|input	指定修改规则的种类
INDEX	指定要设置规则的索引号
accept	允许
drop	丢弃
reject	驳回

【默认状态】

【使用指导】 按指定的索引号设置 firewall|input 规则匹配后的行为为(accept|drop|reject)。

【配置实例】 modify firewall 1 act drop

9.2.17 **modify firewall INDEX act tcpmss**

【命令格式】 modify firewall INDEX act tcpmss <0-9999>

【命令功能】 按指定的索引号设置 firewall 规则匹配后的行为为限制 MSS 并设置其值。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明

INDEX	指定要设置规则的索引号
<0-9999>	tcp mss 的值

【默认状态】

【使用指导】 按指定的索引号设置 firewall 规则匹配后的行为为限制 MSS 并设置其值。设置 tcpmss，需要先将协议设置成 tcp。

【配置实例】 modify firewall 1 act tcpmss 1460

9.2.18 modify snat INDEX nat-ip any

【命令格式】 modify snat INDEX nat-ip any

【命令功能】 按指定的索引号设置 snat 规则 SNAT 的 IP 为隐藏。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
INDEX	指定要设置规则的索引号

【默认状态】

【使用指导】 按指定的索引号设置 snat 规则 SNAT 的 IP 为隐藏。

【配置实例】 modify snat 1 nat-ip any

9.2.19 modify (snat|dnat) INDEX nat-ip

【命令格式】 modify (snat|dnat) INDEX nat-ip single A.B.C.D
modify (snat|dnat) INDEX nat-ip mask A.B.C.D/X.X.X.X
modify (snat|dnat) INDEX nat-ip range A.B.C.D-A.B.C.D

【命令功能】 按指定的索引号设置 snat|dnat 规则 NAT 的 IP。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(snat|dnat)	指定要设置何种规则
INDEX	指定要设置规则的索引号
A.B.C.D	NAT 的 IP 地址
A.B.C.D/X.X.X.X	NAT 的 IP 地址/掩码
A.B.C.D-A.B.C.D	NAT 的 IP 范围

【默认状态】

【使用指导】 按指定的索引号设置 snat|dnat 规则 NAT 的 IP 为指定的 IP 或 IP 范围。

【配置实例】 modify dnat 2 nat-ip single 100.200.10.20
modify dnat 2 nat-ip mask 100.200.10.20/255.255.0.0
modify dnat 2 nat-ip range 100.200.10.20-100.200.10.100

9.2.20 modify (snat|dnat) INDEX nat-port

【命令格式】 modify (snat|dnat) INDEX nat-port any

modify (snat|dnat) INDEX nat-port single <0-65535>
modify (snat|dnat) INDEX nat-port range PORTRANGE

【命令功能】 按指定的索引号设置 snat|dnat 规则 NAT 的端口号。

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(snat|dnat)	指定要设置何种规则
INDEX	指定要设置规则的索引号
any	默认的端口号
<0-65535>	指定的端口号
PORTRANGE	指定的端口号范围，以符号“-”连接两个端口号。

【默认状态】

【使用指导】 按指定的索引号设置 snat|dnat 规则 NAT 的端口号为默认或指定的端口号及范围。设置端口号，需要先将协议设置成 tcp、udp 或者 tcp-and-udp。

【配置实例】 modify snat 1 nat -port any
modify snat 1 nat-port single 100

9.3 显示 Firewall 和 NAT 配置

9.3.1 show (firewall|snat|dnat|input)

【命令格式】 show (firewall|snat|dnat|input) [INDEX]

【命令功能】 按指定的索引号显示 firewall|snat|dnat|input 的规则

【命令模式】 firewall 配置模式

【参数说明】

参数	说明
(firewall|snat|dnat|input)	指定要显示何种规则
INDEX	规则索引号，如果不指定，则显示所有规则

【默认状态】

【使用指导】 按指定的索引号显示 firewall|snat|dnat|input 的规则。

【配置实例】 show snat 1

9.3.2 show firewall-state

【命令格式】 show firewall-state

【命令功能】 显示 firewall 服务运行状态

【命令模式】 firewall 配置模式

【参数说明】 无

【默认状态】

【使用指导】 显示 service enable 表示 firewall 服务正在运行，配置的规则有效；显示 service disable 则相反。

【配置实例】 show firewall-state

10 配置QOS

10.1 QOS 功能简介

QoS 即服务质量，对于网络业务，服务质量包括传输的带宽、传输的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

Qos 技术包括流分类、流量监管、流量整形、端口限速、队列调度等。

10.2 配置 QOS profile

10.2.1 config qos-mode

【命令格式】 **config qos-mode (default|port|flow|hybrid)**

【命令功能】 设置 qos-mode 为端口模式，流模式，混合模式

【命令模式】 配置模式

【参数说明】

参数	说明
port	Qos-mode 为端口模式，不可设置 flow-mode 下的 remap 操作。
flow	Qos-mode 为流模式，不可设置 port-mode 下的 remap 操作。
hybrid	Qos-mode 为混合模式，可以设置端口模式和流模式的 remap 操作。

【使用指导】 使用该命令配置 config qos-mode port。

在系统启动后，必须先设置 qos-mode 才能进行 qos 的 remap 操作，在混合模式下，qos-profile<1-71>给端口的 remap 用，qos-profile <1-64> 给 dscp 映射用，qos-profile <65-72> 给 up 映射用。qos-profile <73-127> 给流的 remap 用。切换模式后，在前一种模式下配置的 qos-profile 等相关的 remap 信息都被清空。

在设置成端口模式或混合模式后，dscp 0

【配置实例】 **config qos-mode hybrid**

10.2.2 **set qos-profile**

【命令格式】 **set qos-profile <1-127>**
【命令功能】 进入 qos profile 配置节点
【命令模式】 配置模式
【参数说明】

参数	说明
1-127	qos profile ID

【使用指导】 使用该命令配置 qos profile。
【配置实例】 **set qos-profile 5**

10.2.3 **qos-profile attributes**

【命令格式】 dp <0-1> up <0-7> tc <0-7> dscp <0-63>
【命令功能】 设置 qos profile 属性
【命令模式】 qos profile 配置模式
【参数说明】

参数	说明
0-1	Drop precedence 取值范围。0 表示 green，1 表示 Red
0-7	User priority（用户优先级）取值范围
0-7	Traffic class，8 个出口队列
0-63	Dscp 取值范围，支持 64 个 dscp 值

【使用指导】 使用该命令配置 qos profile。
【配置实例】 dp 1 up 2 tc 3 dscp 4 （丢弃优先级为 red，用户优先级为 2，tc 为队列 3，dscp 值为 4）

10.2.4 **delete qos-profile**

【命令格式】 **delete qos-profile <1-127>**
【命令功能】 删除已配置的 qos profile
【命令模式】 配置模式
【参数说明】

参数	说明
1-127	设备支持 127 个 qos profile

【使用指导】 使用该命令删除已配置的 qos profile

【配置实例】　delete　qos-profile 100

10.2.5 up-qos-profile mapping

【命令格式】　set up-to-profile <0-7> <1-127>
【命令功能】　根据接收到的 vlan-tagged 报文中的 up 映射为 qos profile 表中的 up
【命令模式】　配置模式
【参数说明】

参数	说明
0-7	User priority（用户优先级）取值范围
1-127	Qos profile 取值范围，Qos mode 为 hybrid 时 Qos profile 的取值范围为 65-72

【使用指导】　使用该命令配置 up-qosProfile maping
【配置实例】　set　up-to-profile　4　65

10.2.6 delete up-qos-profile mapping

【命令格式】　delete　up-to-profile <0-7>
【命令功能】　删除 up 和 qos profile 的对应关系
【命令模式】　配置模式
【参数说明】

参数	说明
0-7	User priority（用户优先级）取值范围

【使用指导】　使用该命令删除 up 和 qos profile 的对应关系
【配置实例】　delete　up-to-profile　4

10.2.7 dscp-qos-profile mapping

【命令格式】　set dscp-to-profile <0-63> <1-127>
【命令功能】　根据接收到的 ip 报文中的 dscp 映射为 qos profile 表中的 dscp
【命令模式】　配置模式
【参数说明】

参数	说明
0-63	DSCP 取值范围

1-127	Qos profile 取值范围，Qos mode 为 hybrid 时 Qos profile 取值范围为 1-64

【使用指导】　使用该命令配置 dscp-qosProfile maping
【配置实例】　set　dscp-to-profile　4　127

10.2.8 **delete dscp-qos-profile mapping**

【命令格式】　delete　dscp-to-profile　<0-63>
【命令功能】　删除 dscp 和 qos profile 的对应关系
【命令模式】　配置模式
【参数说明】

参数	说明
0-63	DSCP 取值范围

【使用指导】　使用该命令删除 dscp 和 qos profile 的对应关系
【配置实例】　delete　dscp-to-profile　4

10.2.9 **dscp-dscp remapping**

【命令格式】　set dscp-to-dscp <0-63> <0-63>
【命令功能】　根据接收到的 ip 报文中的 dscp 映射为一个新的 dscp，再去索引 qos profile
【命令模式】　配置模式
【参数说明】

参数	说明
0-63	DSCP 取值范围，前一个参数指报文中的 dscp 值，后一个参数指映射的值

【使用指导】　使用该命令配置 dscp-dscp　remaping
【配置实例】　set　dscp-to-dscp　5　8

10.2.10 **delete dscp-dscp remapping**

【命令格式】　delete　dscp-to-dscp <0-63>
【命令功能】　取消 dscp 映射成一个新的 dscp 值
【命令模式】　配置模式
【参数说明】

参数	说明

0-63	DSCP 取值范围

【使用指导】　使用该命令取消 dscp 映射成一个新的 dscp 值
【配置实例】　delete　dscp-to-dscp　5

10.2.11　**show qos-profile**

【命令格式】　**show qos-profile**
【命令功能】　显示已配置的 qos profile 内容
【命令模式】　配置模式
【参数说明】　无
【使用指导】　使用该命令显示已配置的 qos profile 明细。DP，UP，DSCP，TC
【配置实例】　show　qos-profile

10.2.12　**show qos-mode**

【命令格式】　**show qos-mode**
【命令功能】　显示 qos 模式信息
【命令模式】　配置模式
【参数说明】　无
【使用指导】　无
【配置实例】　**show qos-mode**

10.2.13　**show remap-table**

【命令格式】　**show remap-table**
【命令功能】　显示配置的 up-profile，dscp-profile 的 mapping table，以及 dscp-dscp remapping table
【命令模式】　配置模式
【参数说明】　无
【使用指导】　显示已配置的 mapping table
【配置实例】　**show remap-table**

10.3　配置 policy-map

10.3.1　**create policy-map**

【命令格式】　create policy-map <1-1000>
【命令功能】　创建一个 policy map
【命令模式】　配置模式
【参数说明】

参数	说明
1-1000	Policy map 取值范围

【使用指导】 使用该命令创建一个 policy map。

【配置实例】 create policy-map 100

10.3.2 delete policy-map

【命令格式】 **delete policy-map <1-1000>**

【命令功能】 删除已创建的 policy map

【命令模式】 配置模式

【参数说明】

参数	说明
1-1000	Policy map ID

【使用指导】 删除已配置的 policy map，前提是未绑定到端口。

【配置实例】 **delete policy-map 100**

10.3.3 config policy-map

【命令格式】 config policy-map <1-1000>

【命令功能】 进入 policy map 节点配置 policy map

【命令模式】 配置模式

【参数说明】

参数	说明
1-1000	Policy map 取值范围

【使用指导】 使用该命令配置已创建的 policy map。和端口绑定才能实现功能。Policymap 配置模式下的命令最终与端口交互。

【配置实例】 config policy-map 100

10.3.4 config qos-markers

【命令格式】 config qos-markers (enable|disable)

【命令功能】 允许或者禁止入口引擎其他的 marker 修改 QOS 属性。

【命令模式】 policy map 配置模式

【默认参数】 enable

【参数说明】

参数	说明
Enable	允许入口引擎其他的 markers 修改 qos 属性

Disable	不允许入口引擎其他的 markers 修改 qos 属性

【使用指导】 入口引擎有很多 markers 可对接收到的报文进行 qos 初始化。例如基于端口的 QOS 初始化，基于 ACL 的初始化。如果一旦该位设置为 disable，则不允许另外 marker 对 QOS 属性进行修改。相反，如果该位设为 enable，则 QOS 属性可能被随后的处理 markers 覆盖。

【配置实例】 config qos-markers disable

10.3.5 trust-mode layer2

【命令格式】 trust-mode l2 up (enable|disable)

【命令功能】 设置二层端口信任模式

【命令模式】 policy map 配置模式

【参数说明】

参数	说明
Enable	二层信任模式，up 可修改
Disable	二层信任模式，up 不可修改

【使用指导】 由于 policy map 最终与端口绑定，所以实际上是配置端口的信任模式和 up 可修改状态。如果配置为二层信任模式，如果报文是 vlan-tagged，则根据 tag 中的 up 值索引 up-to-profile 表中 qos profile 表，改变为相应的 up 值。如果报文非 vlan-tagged，则根据此默认的 qos –profile 值索引改变相应的 up 值

【配置实例】 trust-mode l2 up enable

10.3.6 trust-mode layer3

【命令格式】 trust-mode l3 dscp (enable|disable) remap (enable|disable)

【命令功能】 设置三层端口信任模式

【命令模式】 policy map 配置模式

【参数说明】

参数	说明
Enable	三层信任模式，dscp 可修改，可 remap
Disable	三层信任模式，dscp 不可修改，不允许 remap

【使用指导】 由于 policy map 最终与端口绑定，所以实际上是配置端口的信任模式和 dscp 可修改状态与 remap 状态。如果配置为三层信任模式，如果报文是 ipv4/ipv6，则根据其 dscp 值索引 dscp-to-profile 表中 qos profile 标，改变相应的 dscp 值。此时如果使能 remap，即取其 dscp 值镜像为一个新的 dscp 值，并索引 dscp-to-profile 表，改变相应的

dscp 值。如果报文非 ipv4/ipv6，则根据默认的 qosprofile 表改变相应的值

【配置实例】 trust-mode l3 dscp enable remap enable

10.3.7 trust-mode layer2+layer3

【命令格式】 trust-mode l2+l3 up (enable|disable) dscp (enable|disable remap (enable|disable)

【命令功能】 设置二层+三层端口信任模式

【命令模式】 policy map 配置模式

【参数说明】

参数	说明
Enable	Up 可修改，dscp 可修改，remap 可修改
Disable	Up 不可修改，dscp 不可修改，不允许 remap

【使用指导】 由于 policy map 最终与端口绑定，所以实际上是配置端口的信任模式和 up 可修改状态，dscp 可修改状态与 remap 状态。详见 10.5.5，10.5.6

【配置实例】 trust-mode l2+l3 up enable dscp enable remap enable

10.3.8 show policy-map

【命令格式】 **show policy-map**

【命令功能】 显示 policy map 内容

【命令模式】 配置模式

【参数说明】 无

【使用指导】 显示 policy map 细节。包括默认端口 qos profile index，端口信任模式， up，dscp 可修改状态等等

【配置实例】 **show policy-map**

10.4 绑定端口的 policy map

10.4.1 bind policy map

【命令格式】 bind policy-map <1-1000>

【命令功能】 绑定 policy map 到端口

【命令模式】 端口配置模式

【参数说明】

参数	说明
1-1000	Policy mapID

【使用指导】　绑定已配置的 policy map 到端口上，实现基于端口的 qos 初始化
【配置实例】　bind policy-map 100

10.4.2 unbind policy map

【命令格式】　unbind policy-map <1-1000>
【命令功能】　解除绑定 policy map 与端口的关系
【命令模式】　端口配置模式
【参数说明】

参数	说明
1-1000	Policy mapID

【使用指导】　解除绑定到端口的 policy map
【配置实例】　unbind policy-map 100

10.4.3 show port-qos

【命令格式】　show port-qos
【命令功能】　显示端口的 QOS 信息
【命令模式】　端口配置模式
【参数说明】　无
【使用指导】　显示端口 QOS 的绑定的 policy map index。
【配置实例】　show port-qos

10.5 配置流量监管

流量监管指通过对端口进行监督限制数据流量，丢弃超出限额的流量数据或放入缓冲队列，防止端口流量过大引发网络阻塞。流量监管一般采用令牌桶对流量进行评估。

令牌桶这种控制机制基于令牌桶中是否存在令牌来指示什么时候可以发送流量。令牌桶中的每一个令牌都代表一个字节。如果令牌桶中存在令牌，则允许发送流量；而如果令牌桶中不存在令牌，则不允许发送流量。因此，如果突发门限被合理地配置并且令牌桶中有足够的令牌，那么流量就可以以峰值速率发送。

Policer 创建删除时需注意：policer-range 创建时只能以单个创建的 policer 为样本，不能以批量创建的 policer 为样本；policer-range 创建后不能单个删除，也不能将两个批量创建的连续的 policer 批量删除；作为样本的 policer，在以它为样本批量创建的 policer 未删除前不能删除。

10.5.1 set policer

【命令格式】　set policer <1-255>
【命令功能】　配置流量监管的 policer，进入 policer 节点

【命令模式】 配置模式

【参数说明】

参数	说明
1-255	Policer 取值范围

【使用指导】 配置 policer

【配置实例】 set policer 8

10.5.2 policer CIR CBS

【命令格式】 policer cir <1-100000000> cbs <1-2000000000>

【命令功能】 配置承诺信息速率（committed information rate）,承诺突发量(committed burst size)

【命令模式】 policer 配置模式

【参数说明】

参数	说明
1-100000000	cir 取值范围 （kbps）
1-2000000000	Cbs 取值范围（byte）

【使用指导】 配置 cir，cbs

【配置实例】 policer cir 100 cbs 200000000

10.5.3 config out profile

【命令格式】 config out-profile

【命令功能】 进入 out profile 配置节点配置报文为 non conforming 时的处理方法

【命令模式】 policer 配置模式

【参数说明】 若不进行配置，则默认为 keep

【使用指导】 超出所限制的 cir，cbs 的报文归类为 non-conforming。

【配置实例】 config out-profile

10.5.4 keep

【命令格式】 keep

【命令功能】 保留 non conforming 报文的属性

【命令模式】 out profile 配置模式

【参数说明】 无

【使用指导】 超出所限制的 cir，cbs 的报文归类为 non-conforming，不丢弃报文

【配置实例】 keep

10.5.5 drop

【命令格式】 drop

【命令功能】 丢弃 non conforming 报文

【命令模式】 out profile 配置模式

【参数说明】 无
【使用指导】 超出所限制的 cir，cbs 的报文归类为 non-conforming，丢弃报文
【配置实例】 drop

10.5.6 **remap**

【命令格式】 remap <1-127>
【命令功能】 重新分配属性给 non conforming 报文
【命令模式】 out profile 配置模式
【参数说明】

参数	说明
1-127	Qos profile 取值范围

【使用指导】 超出所限制的 cir，cbs 的报文归类为 non-conforming，重新分配属性
【配置实例】 remap 10

10.5.7 **strict mode**

【命令格式】 policer strict packetsize (l1|l2|l3)
【命令功能】 配置流量监管模式为 strict 的属性，报文字节大小
【命令模式】 配置模式
【默认参数】 l1
【参数说明】

参数	说明
L1	preamble+IPG+CRC
L2	L2+L3+header+CRC
L3	L3+packet without CRC

【使用指导】 监管模式为 strict，即令牌桶令牌数大于报文的字节数，报文定义为 non-conforming
【配置实例】 policer strict packetsize l1

10.5.8 **loose mode**

【命令格式】 policer loose mru <0-2>
【命令功能】 配置流量监管模式为 loose 的属性，mru 大小
【命令模式】 配置模式
【默认参数】 默认情况下，mru 为 0
【参数说明】

参数	说明
0	1.5K
1	2K

2	10K

【使用指导】 监管模式为 loose，即令牌桶令牌数大于令牌桶的 MRU(最大接收单元)，，报文定义为 non-conforming

【配置实例】 policer loose mru 2

10.5.9 enable policer

【命令格式】 policer <1-255> (enable|disable)

【命令功能】 使能/禁用已配置的 policer

【命令模式】 配置模式

【默认参数】 enable

【参数说明】

参数	说明
1-255	Policer 取值范围
Enable	使能 policer
Disable	禁用 policer

【使用指导】 配置 policer 须 disable policer。使能 policer 后，返回硬件处理后实际的 cir，cbs

【配置实例】 policer 4 enable

10.5.10 policer-range

【命令格式】 policer-range <1-255> <1-255> alias <1-255>

【命令功能】 批量创建 policer

【命令模式】 配置模式

【参数说明】

参数	说明
1-255	起始 policer ID
1-255	终止 policer ID
1-255	创建样本的 policer ID

【使用指导】 批量创建 policer，创建范围终止 ID 要比起始 ID 大

【配置实例】 policer-range 1 5 alias 25

10.5.11 delete policer

【命令格式】 delete policer <1-255>

【命令功能】 删除已配置的 policer

【命令模式】 配置模式

【参数说明】

参数	说明
1-255	支持 255 个 policer

【使用指导】 删除已配置的 policer
【配置实例】 **delete policer 7**

10.5.12 delete policer-range

【命令格式】 delete policer-range <1-255> <1-255>
【命令功能】 批量删除 policer
【命令模式】 配置模式
【参数说明】

参数	说明
1-255	起始 policer ID
1-255	终止 policer ID

【使用指导】 批量删除 policer，删除范围的起始终止 ID 需和创建时相同
【配置实例】 delete policer-range 1 5

10.5.13 show policer

【命令格式】 show policer
【命令功能】 显示已配置的 policer
【命令模式】 配置模式
【参数说明】 无
【使用指导】 显示已配置的 policer
【配置实例】 **show policer**

10.6 配置流量整形

流量整形是对输出报文的速率进行控制，使报文以均匀的速率发送出去。流量整形通常是为了使报文速率与下游设备相匹配，以避免不必要的报文丢弃和拥塞。它和流量监管的主要区别在于：流量整形是缓存超过速率限制的报文，使报文以均匀的速率发送出去；而流量监管则是丢弃超过流量速率限制的报文。但是流量整形会增加延迟，而流量监管不会引入额外的延迟。

10.6.1 traffic-shape MAXRATE

【命令格式】 traffic-shape MAXRATE（m|k）BURSTSIZE
【命令功能】 配置基于端口的流量整形

【命令模式】　端口配置模式
【参数说明】

参数	说明
MAXRATE	最大速率
BURSTSIZE	最大 burst，取值范围 1-4096，unit 为 4KB。

【使用指导】　burstsize 为 BURSTSIZE*4KB，突发尺寸。k，表示 64kbps, m 表示 1mbps，下同。
【默认参数】　默认 maxrate 为 0，burstsize 为 0
【配置实例】　traffic-shape 1000 k 4

10.6.2 delete traffic-shape port

【命令格式】　delete traffic-shape port
【命令功能】　删除基于端口的流量整形
【命令模式】　端口配置模式
【参数说明】　无
【使用指导】　删除基于端口的流量整形信息，但是不删除端口上队列的流量整形
【配置实例】　delete　traffic-shape port

10.6.3 traffic-shape queue <0-7> MAXRATE

【命令格式】　traffic-shape queue <0-7> MAXRATE（m|k）BURSTSIZE
【命令功能】　配置基于端口队列的流量整形
【命令模式】　端口配置模式
【参数说明】

参数	说明
0-7	端口支持 8 个出口队列
MAXRATE	最大速率
BURSTSIZE	最大 burst，取值范围 1-4096，unit 为 4KB。

【使用指导】　burstsize 为 BURSTSIZE*4KB. 突发尺寸
【默认参数】　默认情况下，每个队列上的 rate 和 burst 为 0
【配置实例】　traffic-shape queue 5 1000 k 4

10.6.4 delete traffic-shape queue

【命令格式】　delete traffic-shape queue <0-7>
【命令功能】　删除基于端口队列的流量整形
【命令模式】　端口配置模式

【参数说明】

参数	说明
0-7	端口支持 8 个出口队列

【使用指导】 删除端口上队列的流量整形信息，但是不删除基于端口的流量整形

【配置实例】 delete traffic-shape queue 5

10.6.5 show traffic-shape

【命令格式】 show traffic-shape

【命令功能】 显示端口上的流量整形信息

【命令模式】 端口配置模式

【参数说明】 无

【使用指导】 显示端口上流量整形信息，允许流量整形状态，端口和端口上的 8 个队列上的最大速率 rate，最大突发量 burst

【配置实例】 show traffic-shape

10.7 配置队列调度算法

队列调度指使用队列算法对流量进行分类，然后用某种优先级算法将流量发送出去。队列算法都是用以解决特定的网络流量问题，并对宽带资源的分配、延迟、抖动有着十分重要的影响。

队列调度对不同优先级的报文进行分级处理，优先级高的会得到优先发送。常用的队列有：严格优先级 SP(Strict Priority)队列、加权轮询 WRR(Weighted Round Robin)队列、SP+WRR 混合队列。

SP 队列是针对关键业务类型应用设计的。关键业务有一个重要的特点，即在拥塞发生是要求优先获得服务以减小相应的延迟。在 SP 队列调度时，严格按照优先级从高到低的次序优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组，这样，将关键业务的分组放入较高优先级的队列，将非关键业务的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。SP 队列的缺点是：拥堵发生时，如果较高优先级队列中长时间有分组存在，那么低优先级队列中的报文一直得不到服务。

WRR 队列在队列之间进行轮流调度，保证每个队列都得到一定的服务时间。以端口有 8 个输出队列为例，WRR 可为每个队列配置一个加权值（依次为 w7、w6、w5、w4、w3、w2、w1、w0），加权值表示获取资源的比重。如一个 100Mbps 的端口，配置它的 WRR 队列的加权值为 5、5、3、3、1、1、1、1，这样可以保证最低优先级队列至少获得 5Mbps 的带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。WRR 队列还有一个优点是，虽然多个队列的调度是轮询进行的，但对每个队列不是固定地分配服务时间片，如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

SP+WRR 队列时用户可以根据需要配置端口上的部分队列使用 SP 队列调度，部分队列使用 WRR 队列调度，通过在端口上的队列分别加入 SP 调度组和 WRR 调度组，实现 SP+WRR 的调度功能。在队列调度时，系统会优先保证 SP 调度组内的队列调度，当 SP 调度组内的队列没有报文发送时，才会调度 WRR 调度组内的队列。SP 调度组内各个队列执行严格优先级

调度方式，WRR 调度组内各个队列执行加权轮询调度方式。

默认情况下，全局队列调度模式为 wrr，权值为{1,2,3,4,5,6,7,8}.在 sp+wrr 模式下，除了加入到 group 的队列，其他队列默认为 sp 调度。在 wrr 模式下，除了加入到 group 的队列，其他队列默认在 group1 内，且权值为默认值。

10.7.1 queue-scheduler sp

【命令格式】 queue-scheduler sp
【命令功能】 配置队列调度模式为 sp
【命令模式】 配置模式
【参数说明】 无
【使用指导】 配置全局队列调度模式为 sp。
【配置实例】 queue-scheduler sp

10.7.2 queue-scheduler wrr

【命令格式】 queue-scheduler wrr
【命令功能】 配置队列调度模式为 wrr 并进入队列调度配置模式
【命令模式】 配置模式
【参数说明】 无
【使用指导】 配置全局队列调度模式为 wrr
【配置实例】 queue-scheduler wrr

10.7.3 queue-scheduler hybrid

【命令格式】 queue-scheduler hybrid
【命令功能】 配置队列调度模式为 sp+wrr 混合模式并进入队列调度配置模式
【命令模式】 配置模式
【参数说明】 无
【使用指导】 配置全局队列调度模式为 sp+wrr
【配置实例】 queue-scheduler hybrid

10.7.4 wrr (group1|group2) <0-7> <1-255> sp

【命令格式】 wrr (group1|group2) <0-7> <1-255> sp
【命令功能】 当队列调度模式为 sp+wrr 或者 wrr 时，将队列 0-7 加入 group1 或 group2。
【命令模式】 队列调度配置模式
【参数说明】

参数	说明
Group1	Wrr 算法支持两个 group
Group2	Wrr 算法支持两个 group
0-7	队列 0-7

1-255	分配给每个队列的权值

【使用指导】 建议相连的队列放在一个 group 内。

【配置实例】 wrr group1 0 255

10.7.5 show queue-scheduler

【命令格式】 show queue-scheduler

【命令功能】 显示队列调度模式

【命令模式】 配置模式

【参数说明】 无

【使用指导】 显示每个队列的权值和所属 group

【配置实例】 show queue-scheduler