

目 录

第 1 章 ACL 配置命令.....	1
1.1 absolute-periodic/periodic.....	1
1.2 absolute start.....	2
1.3 access-list deny-preemption.....	2
1.4 access-list(ip extended).....	2
1.5 access-list(ip standard).....	4
1.6 access-list(mac extended).....	4
1.7 access-list(mac-ip extended).....	5
1.8 access-list(mac standard).....	7
1.9 clear access-group (in out) statistic interface.....	7
1.10 firewall.....	7
1.11 ip access extended.....	8
1.12 ip access standard.....	8
1.13 ipv6 access-list.....	8
1.14 ipv6 access standard.....	9
1.15 ipv6 access extended.....	10
1.16 {ip ipv6 mac mac-ip} access-group.....	10
1.17 {ip ipv6 mac mac-ip} access-group（接口模式）.....	11
1.18 mac access extended.....	11
1.19 mac-ip access extended.....	11
1.20 permit deny(ip extended).....	12
1.21 permit deny(ip standard).....	13
1.22 permit deny(ipv6 extended).....	13
1.23 permit deny(ipv6 standard).....	14
1.24 permit deny(mac extended).....	14
1.25 permit deny(mac-ip extended).....	16
1.26 show access-lists.....	18
1.27 show access-group.....	19
1.28 show acl vlan-division <vlan-id> to <vlan-id>.....	19

1.29 show firewall.....	19
1.30 show ipv6 access-lists.....	20
1.31 show time-range.....	20
1.32 time-range.....	21
第 2 章 自定义 ACL 命令.....	1
2.1 permit deny.....	1
2.2 udf-access-list standard.....	1
2.3 userdefined-access-list standard offset.....	2
2.4 userdefined-access-list extended offset.....	2
2.5 userdefined-access-list standard.....	2
2.6 userdefined-access-list extended.....	3
2.7 userdefined access-group.....	3
2.8 vaci userdefined access-group.....	4
第 3 章 802.1x 配置命令.....	1
3.1 authentication dot1x radius none.....	1
3.2 debug dot1x detail.....	1
3.3 debug dot1x error.....	1
3.4 debug dot1x fsm.....	2
3.5 debug dot1x packet.....	2
3.6 dot1x accept-mac.....	2
3.7 dot1x eap or enable.....	3
3.8 dot1x enable.....	3
3.9 dot1x dhcp passthrough.....	4
3.10 dot1x guest-vlan.....	4
3.11 dot1x macfilter enable.....	5
3.12 dot1x macbased guest-vlan.....	5
3.13 dot1x macbased port-down-flush.....	5
3.14 dot1x max-req.....	6
3.15 dot1x user allow-movement.....	6
3.16 free-resource destination.....	6
3.17 dot1x max-user macbased.....	7

3.18 dot1x max-user userbased.....	7
3.19 dot1x portbased mode single-mode.....	7
3.20 dot1x port-control.....	7
3.21 dot1x port-method.....	7
3.22 dot1x privateclient enable.....	7
3.23 dot1x privateclient protect enable.....	7
3.24 dot1x re-authenticate.....	7
3.25 dot1x re-authentication.....	8
3.26 dot1x timeout quiet-period.....	8
3.27 dot1x timeout re-authperiod.....	8
3.28 dot1x timeout tx-period.....	9
3.29 dot1x unicast enable.....	9
3.30 dot1x web authentication enable.....	9
3.31 dot1x web authentication ipv6 passthrough.....	9
3.32 dot1x web redirect.....	10
3.33 dot1x web redirect enable.....	10
3.34 free-mac.....	10
3.35 show dot1x.....	10
3.36 show dot1x user.....	12
3.37 clear dot1x.....	12
3.38 user-control limit.....	13
3.39 user-control limit ipv6.....	13
3.40 vlan-pool.....	13
 第 4 章 端口、VLAN 中 MAC、IP 数量限制命令.....	 1
4.1 debug ip arp count.....	1
4.2 debug ipv6 nd count.....	1
4.3 debug switchport arp count.....	1
4.4 debug switchport mac count.....	2
4.5 debug switchport nd count.....	2
4.6 debug vlan mac count.....	2
4.7 ip arp dynamic maximum.....	2

4.8 ipv6 nd dynamic maximum.....	3
4.9 mac-address query timeout.....	3
4.10 show arp-dynamic count.....	3
4.11 show mac-address dynamic count.....	4
4.12 show nd-dynamic count.....	4
4.13 switchport arp dynamic maximum.....	4
4.14 switchport mac-address dynamic maximum.....	5
4.15 switchport mac-address violation.....	5
4.16 switchport nd dynamic maximum.....	5
4.17 vlan mac-address dynamic maximum.....	5
第 5 章 AM 配置命令.....	1
5.1 am enable.....	1
5.2 am port.....	1
5.3 am ip-pool.....	1
5.4 am mac-ip-pool.....	2
5.5 no am all.....	2
5.6 show am.....	2
第 6 章 安全特性配置命令.....	1
6.1 dosattack-check srcip-equal-dstip enable.....	1
6.2 dosattack-check ipv4-first-fragment enable.....	1
6.3 dosattack-check tcp-flags enable.....	1
6.4 dosattack-check srcport-equal-dstport enable.....	2
6.5 dosattack-check tcp-fragment enable.....	2
6.6 dosattack-check tcp-segment.....	2
6.7 dosattack-check icmp-attacking enable.....	3
6.8 dosattack-check icmpV4-size.....	3
6.9 dosattack-check icmpv6-size.....	3
第 7 章 TACACS+命令.....	1
7.1 tacacs-server authentication host.....	1
7.2 tacacs-server key.....	1

7.3 tacacs-server nas-ipv4.....	2
7.4 tacacs-server timeout.....	2
7.5 debug tacacs-server.....	2
第 8 章 RADIUS 配置命令.....	1
8.1 aaa enable.....	1
8.2 aaa-accounting enable.....	1
8.3 aaa-accounting update.....	1
8.4 aaa group server radius.....	2
8.5 debug aaa packet.....	2
8.6 debug aaa detail attribute.....	2
8.7 debug aaa detail connection.....	3
8.8 debug aaa detail escape.....	3
8.9 debug aaa detail event.....	3
8.10 debug aaa error.....	4
8.11 radius nas-ipv4.....	4
8.12 radius nas-ipv6.....	4
8.13 radius-server accounting host.....	5
8.14 radius-server authentication host.....	5
8.15 radius-server dead-time.....	6
8.16 radius-server key.....	6
8.17 radius-server retransmit.....	7
8.18 radius-server timeout.....	7
8.19 radius-server accounting-interim-update timeout.....	7
8.20 server.....	8
8.21 show aaa authenticated-user.....	8
8.22 show aaa authenticating-user.....	9
8.23 show aaa config.....	9
8.24 show radius authenticated-user count.....	10
8.25 show radius authenticating-user count.....	10
8.26 radius 逃生.....	10
8.26.1 radius-server escape { enable disable}.....	10
8.26.2 radius-server escape detection-interval.....	11

第 9 章 SSL 配置命令	1
9.1 ip http secure-server.....	1
9.2 ip http secure-port.....	1
9.3 ip http secure- ciphersuite.....	1
9.4 show ip http secure-server status.....	2
9.5 debug ssl.....	2
第 10 章 IPv6 安全 RA 命令	1
10.1 ipv6 security-ra enable.....	1
10.2 ipv6 security-ra enable.....	1
10.3 show ipv6 security-ra.....	1
10.4 debug ipv6 security-ra.....	2
第 11 章 VLAN-ACL 配置命令	1
11.1 clear vACL statistic VLAN.....	1
11.2 show vACL VLAN.....	1
11.3 vACL ip access-group.....	2
11.4 vACL ipv6 access-group.....	3
11.5 vACL mac access-group.....	3
11.6 vACL mac-ip access-group.....	3
第 12 章 SAVI 配置命令	1
12.1 SAVI 配置命令.....	1
12.1.1 ipv6 cps prefix.....	1
12.1.2 ipv6 cps prefix check enable.....	1
12.1.3 ipv6 dhcp snooping trust.....	1
12.1.4 ipv6 nd snooping trust.....	2
12.1.5 savi check binding.....	2
12.1.6 savi enable.....	2
12.1.7 savi ipv6 binding num.....	3
12.1.8 savi ipv6 check source binding.....	3
12.1.9 savi ipv6 check source ip-address mac-address.....	4
12.1.10 savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable.....	4
12.1.11 savi ipv6 mac-binding-limit.....	5
12.1.12 savi max-dad-delay.....	5
12.1.13 savi max-dad-prepare-delay.....	5

12.1.14 savi max-slaac-life.....	5
12.1.15 savi timeout bind-protect.....	6
12.2 SAVI 监控和调试命令.....	6
12.2.1 监控和调试信息.....	6
第 13 章 Captive Portal 认证命令.....	1
13.1 认证功能命令.....	1
13.1.1 ac-name.....	1
13.1.2 authentication roam enable.....	1
13.1.3 captive-portal.....	1
13.1.4 captive-portal binding arp（暂不支持）.....	2
13.1.5 captive-portal client deauthenticate.....	2
13.1.6 captive-portal client re-auth log { enable disable }.....	3
13.1.7 captive-portal client keep-alive flow-detection enable.....	3
13.1.8 captive-portal client keep-alive flow-detection interval.....	3
13.1.9 captive-portal client keep-alive flow-detection number.....	4
13.1.10 clear.....	4
13.1.11 configuration.....	4
13.1.12 debug captive-portal packet.....	5
13.1.13 debug captive-portal trace.....	5
13.1.14 debug captive-portal alive-detail.....	5
13.1.15 debug captive-portal alive-status.....	5
13.1.16 debug captive-portal alive-time.....	6
13.1.17 debug captive-portal error.....	6
13.1.18 enable (全局).....	6
13.1.19 enable (例程).....	7
13.1.20 external portal-server server-name.....	7
13.1.21 http-redirect-filter <1-32> {ip A.B.C.D domain WORD}.....	7
13.1.22 http-redirect-filter <1-32>.....	8
13.1.23 name.....	8
13.1.24 nas-ipv4.....	8
13.1.25 portal enable configuration <id> [vlan-pool WORD].....	9
13.1.26 portal-server.....	9
13.1.27 radius accounting.....	9
13.1.28 radius-accounting update interval.....	10
13.1.29 radius-acct-server.....	10
13.1.30 radius-auth-server.....	10
13.1.31 redirect url-head <word>.....	11
13.1.32 redirect attribute ssid enable.....	11
13.1.33 redirect attribute ssid name.....	11
13.1.34 redirect attribute nas-ip enable.....	12
13.1.35 redirect attribute nas-ip name.....	12

13.1.36	vlan-pool <1-255> <WORD>.....	12
13.1.37	session-timeout.....	13
13.1.38	show captive-portal.....	13
13.1.39	show captive-portal status.....	13
13.1.40	show captive-portal configuration.....	14
13.1.41	show captive-portal configuration interface.....	14
13.1.42	show captive-portal configuration status.....	15
13.1.43	show captive-portal client status.....	15
13.1.44	show captive-portal configuration client.....	16
13.1.45	show captive-portal ext-portal-server status.....	16
13.1.46	show captive-portal interface configuration status.....	16
13.2	Free-resource 命令.....	17
13.2.1	free-resource (全局)	17
13.3	认证白名单.....	17
13.3.1	free-mac.....	17
13.4	认证成功后页面自动推送命令 (暂不支持).....	18
13.4.1	redirect attribute url-after-login enable.....	18
13.4.2	redirect attribute url-after-login name.....	18
13.4.3	redirect attribute url-after-login encode.....	18
13.4.4	redirect attribute url-after-login value.....	19
13.5	Portal 无感知命令.....	19
13.5.1	fast-mac-auth.....	19
13.6	Portal 逃生命令.....	19
13.6.1	portal-server-detect server-name <name>.....	19
13.6.2	portal-server-detect client-deauth.....	20
13.6.3	show captive-portal ext-portal-server server-name <name> status.....	21

第 1 章 ACL 配置命令

1.1 absolute-periodic/periodic

命令: [no] absolute-periodic {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <start_time> to {Monday | Tuesday | Wednesday | Thursday | Friday | Saturday | Sunday} <end_time>

[no] periodic
 {{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday} | daily | weekdays | weekend} <start_time> to <end_time>

功能: 定义一周内的各种不同要求的时间范围, 每周都循环这个时间。

参数:

Friday Friday(星期五)
Monday Monday (星期一)
Saturday Saturday (星期六)
Sunday Sunday (星期日)
Thursday Thursday (星期四)
Tuesday Tuesday (星期二)
Wednesday Wednesday (星期三)
daily Every day of the week (每天)
weekdays Monday thru Friday (星期一到星期五)
weekend Saturday and Sunday (星期六到星期日)
start_time 开始时间点, HH:MM:SS (小时: 分钟: 秒)
end_time 结束时间点, HH:MM:SS (小时: 分钟: 秒)

注: time-range 轮询时间是 1 分钟一次, 所以时间的误差 ≤ 1 分钟。

命令模式: 时间范围模式

缺省情况: 没有时间范围配置

使用指南: 周期性的时间和日期, 周期是定义每周的 1~6 和周日的具体时间段, 可以同时配置多个周期性时段, 它们之间是“或”的关系。它的形式是:

day1 hh:mm:ss To day2 hh:mm:ss 或者
 {[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To
 hh:mm:ss

举例: 使能在 Tuesday 到 Saturday 内的 9:15:30 到 12:30:00 时间段内配置生效

```
Switch(config)#time-range admin_timer
```

```
Switch(Config-Time-Range-admin_timer)#absolute-periodic tuesday 9:15:30 to saturday 12:30:00
```

使能在 Monday、Wednesday、Friday 和 Sunday 四天内的 14:30:00 到 16:45:00 时间段配置生效

```
Switch (Config-Time-Range-admin_timer)#periodic monday wednesday friday sunday 14:30:00 to 16:45:00
```

1.2 absolute start

命令： [no]absolute start <start_time> <start_data> [end <end_time> <end_data>]

功能： 定义一个绝对时间段，这个时间段是根据本设备的时钟运行。

参数： **start_time** ：开始时间点，HH:MM:SS (小时：分钟：秒)

end_time ：结束时间点，HH:MM:SS (小时：分钟：秒)

start_data ：开始日期，格式是，YYYY.MM.DD (年.月.日) **end_data** ：结束日期，格式是，YYYY.MM.DD (年.月.日)

注：time-range 轮询时间是 1 分钟一次，所以时间的误差≤1 分钟。

命令模式： 时间范围模式

缺省情况： 没有时间范围配置

使用指南： 绝对时间及日期，指定具体开始的年，月，日，小时，分钟，不能配置多个绝对时间及日期，重复配置时，后配置的覆盖以前配置的绝对时间及日期。

举例： 使能在 2004.10.1 到 2005.1.26 内从 6:00:00 到 13:30:00 配置生效

```
Switch(config)#Time-range -admin_timer
```

```
Switch(Config-Time-Range- admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26
```

1.3 access-list deny-preemption

命令： [no] access-list deny-preemption

功能： 开启 deny 优先功能；no 表示关闭 deny 优先功能。

参数： 无。

缺省情况： 默认开启 deny 优先功能。

命令模式： 全局配置模式。

使用指南： 开启 deny 优先功能，保证了 ACL 功能模块与其他的功能模块之间 deny 动作优先的原则，但限制了 ACL 规则的条数。只有在开启 firewall 后才能使用该命令，不然会返回失败；如果已经向硬件下发了 ACL，此时执行该命令会提示重启防火墙后生效。

举例： 关闭 deny 优先功能。

```
Switch(config)#no access-list deny-preemption
```

1.4 access-list(ip extended)

命令： access-list <num> {deny | permit} icmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dlpAddr> <dMask>} | any-destination | {host-destination <dlpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

access-list <num> {deny | permit} igmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dlpAddr> <dMask>} | any-destination | {host-destination <dlpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

access-list <num> {deny | permit} tcp {{<slpAddr> <sMask>} | any-source |

```
{host-source <slpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }]
{{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port
{ <dPort> | range <dPortMin> <dPortMax> }] [ack+ fin+ psh+ rst+ urg+ syn]
[precedence <prec> ] [tos <tos> ] [time-range<time-range-name>]
```

```
access-list <num> {deny | permit} udp {{ <slpAddr> <sMask> } | any-source |
{host-source <slpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }
{{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port
{ <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec> ] [tos <tos> ]
[time-range<time-range-name>]
```

```
access-list <num> {deny | permit} {eigrp | gre | igmp | ipinip | ip | ospf |
<protocol-num> } {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> }}
{{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }}
[precedence <prec> ] [tos <tos> ] [time-range<time-range-name>]
```

```
no access-list <num>
```

功能：创建一条匹配特定 IP 协议或所有 IP 协议的数字扩展 IP 访问列表，如果已有此访问列表，则增加一条 rule 表项；本命令的 no 操作为删除一条数字扩展 IP 访问列表。

参数：<num>为访问表标号，100-299；<protocol>为 ip 上层协议号，0-255；<slpAddr>为源 IP 地址，格式为点分十进制；<sMask>为源 IP 的反掩码，格式为点分十进制；<dIpAddr>为目的 IP 地址，格式为点分十进制；<dMask>为目的 IP 的反掩码，格式为点分十进制，关心的位置 0，忽略的位置 1；<igmp-type>，igmp 的类型，0-15；<icmp-type>，icmp 的类型，0-255；<icmp-code>，icmp 的协议编号，0-255；<prec>，IP 优先级，0-7；<tos>，tos 值，0-15；<sPort>，源端口号，0-65535；<sPortMin>，源端口范围下边界；<sPortMax>，源端口范围上边界；<dPort>，目的端口号，0-65535；<dPortMin>，目的端口范围下边界；<dPortMax>，目的端口范围上边界；<time-range-name>，时间范围名称。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：当用户第一次指定特定<num>时，创建此编号的 ACL，之后在此 ACL 中添加表项；标号为 200-299 访问列表可以配置非连续 IP 地址反掩码。

<igmp-type>代表 IGMP 报文的类型，常用的取值可参照以下的说明：

17(0x11): IGMP QUERY 报文

18(0x12): IGMP V1 REPORT 报文

22(0x16): IGMP V2 REPORT 报文

23(0x17): IGMP V2 LEAVE 报文

34(0x22): IGMP V3 REPORT 报文

19(0x13): DVMRP 报文

20(0x14): PIM V1 报文

特别提示：这里所指的报文类型是指不含有 IP OPTION 情况下的报文类型，在通常情况下，IGMP 报文是包含有 OPTION 字段的，这样的设置对这种报文没有作用。如果希望对包含 OPTION 的报文进行配置，请直接使用配置 OFFSET 的方式进行。

举例：创建编号为 110 的数字扩展访问列表。拒绝 icmp 报文通过，允许目的地址为 192.168.0.1 目的端口为 32 的 udp 包通过。

```
Switch(config)#access-list 110 deny icmp any-source any-destination
```

```
Switch(config)#access-list 110 permit udp any-source host-destination 192.168.0.1 d-port
```

1.5 access-list(ip standard)

命令： access-list <num> {deny | permit} {{<slpAddr> <sMask >} | any-source | {host-source <slpAddr>}}

no access-list <num>

功能： 创建一条数字标准 IP 访问列表，如果已有此访问列表，则增加一条 rule 表项；本命令的 no 操作为删除一条数字标准 IP 访问列表。

参数： <num> 为访问表标号，1-99；<slpAddr> 为源 IP 地址，格式为点分十进制；<sMask > 为源 IP 的反掩码，格式为点分十进制。

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 当用户第一次指定特定 <num> 时，创建此编号的 ACL，之后在此 ACL 中添加表项。

举例： 创建一条编号为 20 的数字标准 IP 访问列表，允许源地址为 10.1.1.0/24 的数据包通过，拒绝其余源地址为 10.1.1.0/16 的数据包通过。

```
Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
```

```
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255
```

1.6 access-list(mac extended)

命令： access-list <num> {deny | permit} {any-source-mac | { host-source-mac <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} {untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3} [<offset1> <length1> <value1> [<offset2> <length2> <value2> [<offset3> <length3> <value3> [<offset4> <length4> <value4>]]]]

no access-list <num>

功能： 定义一条扩展数字 MAC ACL 规则，No 命令删除一个扩展数字 MAC 访问表规则

参数： <num> 访问表号，这是一个从 1100—1199 的十进制号；deny 如果规则匹配，拒绝访问；permit 如果规则匹配，允许访问；<any-source-mac> 任何源地址；<any-destination-mac> 任何目的地址；<host_smac>，<smac> 源 MAC 地址；<smac-mask> 源 MAC 地址的掩码(反掩码)；<host_dmac>，<dmac> 目的 MAC 地址；<dmac-mask> 目的 MAC 地址的掩码(反掩码)；untagged-eth2 未标记的 ethernet II 包格式；tagged-eth2 标记的 ethernet II 包格式；untagged-802-3 未标记的 ethernet 802.3 包格式；tagged-802-3 标记的 ethernet 802.3 包格式。Offset(x) 从包头开始起的偏移量，范围为（12-79），窗口必须从源 MAC 后面开始，从前至后依次配置，并且窗口之间不可重叠，也就是要求：Offset(x+1) 必须大于或等于 Offset(x)+len (x)；Length(x) 长度为 1-4，而且 Offset(x)+Length(x) 必须不大于 80（当前必须不大于 64）；Value(x) 16 进制数表示，取值范围：当 Length(x)=1 为 0-ff，当 Length(x)=2 为 0-ffff，当 Length(x)=3 为 0-ffffff，当 Length(x)=4 为 0-fffffff；

对于 Offset(x)，对不同的数据帧类型，它的取值范围不同：

对 untagged-eth2 类型帧: <12~75>

对 untagged-802.3 类型帧: <20~75>

对 tagged-eth2 类型帧: <12~79>

对 tagged-802.3 类型帧: <12~15> <24~79>

命令模式: 全局配置模式

缺省配置: 没有配置任何的访问列表

使用指南: 当用户第一次指定特定<num>时, 创建此编号的 ACL, 之后在此 ACL 中添加表项。

举例: 允许任意源 MAC 地址任意目的 MAC 地址的 tagged-eth2, 且其第 17 18 个字节分别为 0x08 , 0x0 的包通过。

```
Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2
16 2 0800
```

1.7 access-list(mac-ip extended)

命令:

```
access-list<num>{deny|permit}{any-source-mac|
{host-source-mac<host_smac>}{<smac><smac-mask>}}
{any-destination-mac|{host-destination-mac
<host_dmac>}{<dmac><dmac-mask>}}icmp
{{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|
{host-destination<destination-host-ip>}}[<icmp-type> [<icmp-code>]] [precedence
<precedence>] [tos <tos>][time-range<time-range-name>]
access-list<num>{deny|permit}{any-source-mac|
{host-source-mac<host_smac>}{<smac><smac-mask>}}
{any-destination-mac|{host-destination-mac
<host_dmac>}{<dmac><dmac-mask>}}igmp
{{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|
{host-destination<destination-host-ip>}} [<igmp-type>] [precedence <precedence>]
[tos <tos>][time-range<time-range-name>]
access-list      <num>      {deny|permit}{any-source-mac|      {host-source-mac
<host_smac>      }{{      <smac>      <smac-mask>      }}{any-destination-mac|
{host-destination-mac <host_dmac> }{{ <dmac> <dmac-mask> }}tcp {{ <source>
<source-wildcard> }|any-source| {host-source <source-host-ip> }}[s-port{ <port1> |
range <sPortMin> <sPortMax> }] {{ <destination> <destination-wildcard> } |
any-destination | {host-destination <destination-host-ip> }} [d-port { <port3> | range
<dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence
<precedence> ] [tos <tos> ] [time-range<time-range-name>]
access-list      <num>      {deny|permit}{any-source-mac|      {host-source-mac
<host_smac>      }{{      <smac>      <smac-mask>      }}{any-destination-mac|
{host-destination-mac <host_dmac> }{{ <dmac> <dmac-mask> }}udp {{ <source>
<source-wildcard> }|any-source| {host-source <source-host-ip> }}[s-port{ <port1> |
```

```

range      <sPortMin>      <sPortMax>      ]]      {{      <destination>
<destination-wildcard>      ]any-destination|      {host-destination
<destination-host-ip> }][d-port{ <port3> | range <dPortMin> <dPortMax> }]
[precedence <precedence> ] [tos <tos> ] [time-range<time-range-name>]
access-list <num>      {deny|permit}{any-source-mac|      {host-source-mac
<host_smac>      }|{      <smac>      <smac-mask>      }}
{any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac>
<dmac-mask> }} {eigrp|gre|igrp|ip|ipinip|ospf}{ <protocol-num> }} {{ <source>
<source-wildcard> }|any-source|{host-source <source-host-ip> }} {{ <destination>
<destination-wildcard> }|any-destination| {host-destination <destination-host-ip> }}
[precedence <precedence> ] [tos <tos> ] [time-range<time-range-name>]

```

功能：定义一条扩展数字 MAC-IP ACL 规则，No 命令删除一个扩展数字 MAC-IP ACL 访问表规则

参数：**num** 访问表号。这是一个从 3100—3299 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；**any-source-mac** 任何源 MAC 地址；**any-destination-mac** 任何目的 MAC 地址；**host_smac** , **smac** 源 MAC 地址；**smac-mask** 源 MAC 地址的掩码(反掩码)；**host_dmac** , **dmac** 目的 MAC 地址；**dmac-mask** 目的 MAC 地址的掩码(反掩码)；**protocol** 名字或 IP 协议的号。它可以是关键字 **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **ospf**, **tcp**, **or udp**，也可以是表 IP 协议号的 0 到 255 的一个整数。为了匹配任何 Internet 协议(包括 ICMP, TCP 和 UDP)使用关键字 **ip**；**source-host-ip**, **source** 包发送的源网络或源主机号。32 位二进制数，点分十进制表示；**host-source** 表示地址是源主机 IP 地址，否则是网络 IP 地址；**source-wildcard** 源 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**destination-host-ip**, **destination** 包发送时要去往的目的网络或主机号。32 位二进制数，点分十进制表示；**host-source** 表示地址是目的主机 IP 地址，否则是网络 IP 地址；**destination-wildcard** 目的 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**s-port** (可选) 表示要匹配 TCP/UDP 源端口；**port1** (可选) TCP/UDP 源端口号值，端口号是一个 0 到 65535 的数字；**<sPortMin>**，源端口范围下边界；**<sPortMax>**，源端口范围上边界；**d-port** (可选)表示要匹配 TCP/UDP 目的端口；**port3** (可选)TCP/UDP 目的端口号值，端口号是一个 0 到 65535 的数字；**<dPortMin>**，目的端口范围下边界；**<dPortMax>**，目的端口范围上边界；**[ack] [fin] [psh] [rst] [urg] [syn]**，(可选) 只对 TCP 协议，可选多个标志位，当 TCP 数据报**[ack] [fin] [psh] [rst] [urg] [syn]**的相应位设置时，即初始化 TCP 数据报以形成一个连接时出现匹配；**precedence** (可选) 包可由优先级过滤，为 0 到 7 的数字；**tos** (可选)包可由服务级类型过滤，为 0 到 15 的数字；**icmp-type** (可选) ICMP 包可由 ICMP 报文类型过滤。类型是数字 0 到 255；**icmp-code** (可选) ICMP 包可由 ICMP 报文明码过滤。该代码是数字 0 到 255；**igmp-type** (可选) IGMP 包可由 IGMP 报文类型或报文明码过滤。类型是数字 0 到 15；**<time-range-name>** 时间范围名称。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表。

使用指南：当用户第一次指定特定 **<num>** 时，创建此编号的 ACL，之后在此 ACL 中添加表项；标号为 3200-3299 访问列表可以配置非连续 IP 地址反掩码。

举例：允许源 MAC 为 00-12-34-45-XX-XX，任意目的 MAC 地址，源 IP 地址为：100.1.1.0 0.255.255.255，任意目的 IP 地址，且源端口是 100，目的端口是 40000 的 TCP 报文通过 Switch(config)# access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF

```
any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-port 40000
```

1.8 access-list(mac standard)

命令： `access-list <num> {deny|permit} {any-source-mac | {host-source-mac <host_smac> } | {<smac> <smac-mask> } }`

`no access-list <num>`

功能： 定义一条标准数字 MAC ACL 规则，No 命令删除一个标准数字 MAC 访问表规则

参数： `<num>` 访问表号，这是一个从 700 到 799 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；`<smac>`，`<host_smac>` 源 MAC 地址；`<smac-mask>` 源 MAC 地址的掩码（反掩码）

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 当用户第一次指定特定 `<num>` 时，创建此编号的 ACL，之后在此 ACL 中添加表项。

举例： 允许源 MAC 地址为 00-00-XX-XX-00-01 的数据包通过，拒绝源地址为 00-00-00-XX-00-ab 的数据包通过。

```
Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00
```

```
Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00
```

1.9 clear access-group (in | out) statistic interface

命令： `clear access-group (in | out) statistic interface { <interface-name> | ethernet<interface-name> }`

功能： 清空指定端口的指定方向的包过滤统计信息。

参数： `<interface-name>`：接口名称。

命令模式： 特权用户模式。

缺省情况： 无。

举例： 清空 1/1 接口的包过滤统计信息。

```
Switch#clear access-group out statistic interface ethernet 1/1
```

1.10 firewall

命令： `firewall { enable | disable }`

功能： 允许防火墙起作用或禁止防火墙起作用。

参数： **enable** 表示允许防火墙起作用；**disable** 表示禁止防火墙起作用。

缺省情况： 缺省为防火墙不起作用。

命令模式： 全局配置模式。

使用指南： 在允许和禁止防火墙时，都可以设置访问规则。但只有在防火墙起作用时才可以将规则应用至特定端口。使防火墙不起作用后将删除端口上绑定的所有 ACL。

举例： 允许防火墙起作用。

```
Switch(config)#firewall enable
```

1.11 ip access extended

命令： ip access extended <name>

no ip access extended <name>

功能： 创建一条命名扩展 IP 访问列表；本命令的 no 操作为删除此命名扩展 IP 访问列表（包含所有表项）。

参数： <name>为访问表标名，字符串长度为 1-32，不允许为纯数字序列。

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例： 创建一条名为 tcpFlow 的命名扩展 IP 访问列表。

Switch(config)#ip access-list extended tcpFlow

1.12 ip access standard

命令： ip access standard <name>

no ip access standard <name>

功能： 创建一条命名标准 IP 访问列表；本命令的 no 操作为删除此命名标准 IP 访问列表（包含所有表项）。

参数： <name>为访问表标名，字符串长度为 1-32，不允许为纯数字序列。

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例： 创建一条名为 ipFlow 的命名标准 IP 访问列表。

Switch(config)#ip access-list standard ipFlow

1.13 ipv6 access-list

命令： ipv6 access-list <num-std> {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}}

ipv6 access-list <num-ext> {deny | permit} icmp {{ <sIPv6Prefix/sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

ipv6 access-list <num-ext> {deny | permit} tcp {{ <sIPv6Prefix/<sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIPv6Prefix/<dPrefixlen> } | any-destination | {host-destination <dIPv6Addr> }} [dPort { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <flowlabel>] [time-range<time-range-name>]

ipv6 access-list <num-ext> {deny | permit} udp {{ <sIPv6Prefix/<sPrefixlen> } | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin>

```

<sPortMax> }} {{ <dIPv6Prefix/<dPrefixlen> } | any-destination | {host-destination
<dIPv6Addr> }} [dPort { <dPort> | range <dPortMin> <dPortMax> }} [dscp <dscp> ]
[flow-label <flowlabel> ] [time-range<time-range-name>]
    ipv6 access-list <num-ext> {deny | permit} <next-header>
{ <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> }}
{ <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }}
[dscp <dscp> ] [flow-label <fl> ] [time-range<time-range-name>]
no ipv6 access-list { <num-std> | <num-ext> }

```

功能： 创建一条 IPv6 数字标准访问列表，如果已有此访问列表，则增加一条 rule 表项；本命令的 no 操作为删除一条数字标准 IPv6 访问列表。

参数： **<num-std>** 为访问表标号，取值范围为 500~599； **<num-ext>** 为访问表标号，取值范围为 600~699； **<sIPv6Prefix>** 为源 IPv6 地址前缀， **<sPrefixlen>** 为源 IPv6 地址前缀长度，取值范围为 1~128； **<sIPv6Addr>** 为源 IPv6 地址； **<dIPv6Prefix>** 为目的 IPv6 地址前缀， **<dPrefixlen>** 为目的 IPv6 地址前缀长度，取值范围为 1~128； **<dIPv6Addr>** 为目的 IPv6 地址； **<icmp-type>** icmp 的类型； **<icmp-code>** icmp 的协议编号； **<dscp>** IPv6 优先级，范围为 0~63； **<fl>** 流标签值，范围为 0~1048575； **syn, ack, urg, rst, fin, psh, tcp** 标志位； **<sPort>** 源端口号，范围为 0~65535； **<sPortMin>** 源端口范围下边界； **<sPortMax>** 源端口范围上边界； **<dPort>** 目的端口号，范围为 0~65535； **<dPortMin>** 目的端口范围下边界； **<dPortMax>** 目的端口范围上边界； **<next-header>** IPv6 下一头，范围为 0~255； **<time-range-name>** 时间范围名称。

命令模式： 全局配置模式

缺省情况： 缺省没有配置任何的访问列表。

使用指南： 当用户第一次以特定 **<num>** 创建此编号的 acl，之后则在此 acl 中添加表项。

举例： 创建一条编号为 520 的 IPv6 数字标准访问列表，允许源地址为 2003:1:2:3::1/64 网段的数据包通过，拒绝其余源地址为 2003:1:2::1/48 网段的数据包通过。

```
Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64
```

```
Switch (config)#ipv6 access-list 520 deny 2003:1:2::1/48
```

1.14 ipv6 access standard

命令： **ipv6 access-list standard <name>**

no ipv6 access-list standard <name>

功能： 创建一条 IPv6 命名标准访问列表；本命令的 no 操作为删除此 IPv6 命名标准访问列表（包含所有表项）。

参数： **<name>** 为访问表标名，字符串长度为 1-32。

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例： 创建一条名为 ip6Flow 的命名标准 IPv6 访问列表。

```
Switch(config)#ipv6 access-list standard ip6Flow
```

1.15 ipv6 access extended

命令：ipv6 access-list extended <name>

no ipv6 access-list extended <name>

功能： 创建一条 IPv6 命名扩展访问列表；本命令的 no 操作为删除此 IPv6 命名扩展访问列表。

参数： <name> 为访问表标名，字符串长度为 1～32。

命令模式： 全局配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例： 创建一条名为 tcpFlow 的 IPv6 命名扩展访问列表。

Switch (config)#ipv6 access-list extended tcpFlow

1.16 {ip|ipv6|mac|mac-ip} access-group

命令：{ip|ipv6|mac|mac-ip} access-group <name> {in | out}[traffic-statistic]

no {ip|ipv6|mac|mac-ip} access-group <name> {in | out}

功能： 在端口的某个方向上应用一条 access-list，并且根据可选项决定是否对 ACL 规则加上统计计数器；本命令的 no 操作为删除绑定在端口上的 access-list。

参数： <name>，命名访问表的名字，字符串长度为 1-32。

命令模式： 端口配置模式

缺省情况： 端口没有绑定 ACL。

使用指南： 一个端口可以绑定一条入口和出口规则。Egress ACL 可以在出口和入口方向实现对报文的过滤，符合特定规则的报文可以允许通过或者禁止通过。ACL 可以支持 IP ACL，MAC ACL，MAC-IP ACL，IPv6 ACL。在端口入口方向上可以同时配置四种 ACL；在端口出口方向上由于硬件只有四个资源，IP 和 MAC ACL 各占一个资源，MAC-IP 和 IPv6 ACL 各占两个资源，当硬件资源占满后则无法再配置，即一个端口在出口方向上不能同时配置四种 ACL，同时配置三种 ACL 时也只能是 IP、MAC 和 MAC-IP 类型同时配置或 IP、MAC 和 IPv6 类型同时配置，同时配置两种 ACL 时可以任意选取，没有限制。一种类型的 ACL 在端口上只能配置一条。

目前在端口上绑定 Egress acl 时要注意如下几个方面：

1. 绑定 IP ACL 时不支持绑定匹配 tcp/udp range 的 ACL
2. 绑定 MAC-IP ACL 时不支持绑定匹配 tcp/udp range 的 ACL
3. 绑定 IPv6 ACL 时不支持绑定匹配 flowlabel 的 ACL

基于关心的包头字段 ACL 可以分为四种：MAC ACL，IP ACL，MAC-IP ACL，IPv6 ACL；某种情况下，当一个数据包匹配四条 ACL 中的多条时，ACL 的过滤动作（permit，deny）会发生冲突。基于结果确定性的考虑，为每一种 ACL 指定了严格的优先级。当过滤动作发生冲突时，可以依据优先级决定包过滤的最终动作。

当绑定 ACL 到端口时，有如下限制：

1. 每个端口入口可以绑定一条 MAC-IP ACL，一条 IP ACL，一条 MAC ACL 和一条 IPv6 ACL；
2. 当同时绑定四条 ACL 且数据包同时匹配其中多条 ACL 时，优先关系从高到低如下，如果优先级相同，则先配置的优先级高：

入口 IPv6 ACL
入口 MAC-IP ACL
入口 MAC ACL
入口 IP ACL

举例：将名为 aaa 的访问列表绑定到端口的入方向上。

```
Switch(Config-If-Ethernet1/5)#ip access-group aaa in
```

1.17 {ip|ipv6|mac|mac-ip} access-group（接口模式）

本交换机不支持此命令。

1.18 mac access extended

命令：mac-access-list extended <name>

no mac-access-list extended <name>

功能：定义一个命名方式的 MAC ACL 表或进入访问表配置模式，no 命令删除命名方式的 ACL 表。

参数：<name> 访问表的名字，不包括空格或引号，必须用字母字符开头。长度最大为 32。
（注：大小写敏感）

命令模式：全局配置模式

缺省配置：没有配置任何的访问列表。

使用指南：第一次以调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例：创建一个名字为 mac_acl 的 MAC ACL。

```
Switch(config)# mac-access-list extended mac_acl
```

```
Switch(Config-Mac-Ext-Nacl-mac_acl)#
```

1.19 mac-ip access extended

命令：mac-ip-access-list extended <name>

no mac-ip-access-list extended <name>

功能：定义一个命名方式的 MAC-IP ACL 表或进入访问表配置模式，no 命令删除命名方式的 ACL 表。

参数：name 访问表的名字，不包括空格或引号，必须用字母字符开头。长度最大为 32。
（注：大小写敏感）

命令模式：全局配置模式

缺省情况：没有命名的 MAC-IP 访问表。

使用指南：第一次调用此命令后，只是创建一个空的命名访问列表，其中不包含任何表项。

举例：创建一个名字为 macip_acl 的 MAC-IP ACL。

```
Switch(config)# mac-ip-access-list extended macip_acl
```

```
Switch(Config-MacIp-Ext-Nacl-macip_acl)#
```

1.20 permit | deny(ip extended)

命令：[no] {deny | permit} icmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

[no] {deny | permit} igmp {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range<time-range-name>]

[no] {deny | permit} tcp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

[no] {deny | permit} udp {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{ <slpAddr> <sMask> } | any-source | {host-source <slpAddr> } } {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> } } [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

功能：创建一条匹配特定 IP 协议或所有 IP 协议的命名扩展 IP 访问规则；

参数：<slpAddr>为源 IP 地址，格式为点分十进制；<sMask>为源 IP 的反掩码，格式为点分十进制；<dIpAddr>为目的 IP 地址，格式为点分十进制；<dMask>为目的 IP 的反掩码，格式为点分十进制，关心的位置 0，忽略的位置 1；<igmp-type>，igmp 的类型，0—15；<icmp-type>，icmp 的类型，0—255；<icmp-code>，icmp 的协议编号，0—255；<prec>，IP 优先级，0—7；<tos>，tos 值，0-15；<sPort>，源端口号，0-65535；<sPortMin>，源端口范围下边界；<sPortMax>，源端口范围上边界；<dPort>，目的端口号，0-65535；<dPortMin>，目的端口范围下边界；<dPortMax>，目的端口范围上边界；<time-range-name>，时间范围名称。

命令模式：命名扩展 IP 访问列表配置模式

缺省情况：没有配置任何的访问列表。

使用指南：无。

举例：创建名为 udpFlow 的扩展访问列表。拒绝 igmp 报文通过，允许目的地址为 192.168.0.1 目的端口为 32 的 udp 包通过。

```
Switch(config)#ip access-list extended udpFlow
```

```
Switch(Config-Ext-Nacl-udpFlow)# deny igmp any-source any-destination
```

```
Switch(Config-Ext-Nacl-udpFlow)# permit udp any-source host-destination 192.168.0.1 d-port 32
```

1.21 permit | deny(ip standard)

命令: {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}
no {deny | permit} {{<slpAddr> <sMask>} | any-source | {host-source <slpAddr>}}

功能: 创建一条命名标准 IP 访问规则 (rule); 本命令的 no 操作为删除此命名标准 IP 访问规则 (rule)。

参数: <slpAddr>为源 IP 地址, 格式为点分十进制; <sMask>为源 IP 的反掩码, 格式为点分十进制。

命令模式: 命名标准 Ip 访问列表配置模式

缺省情况: 没有配置任何的访问列表。

使用指南: 无。

举例: 允许源地址为 10.1.1.0/24 的数据包通过, 拒绝其余源地址为 10.1.1.0/16 的数据包通过。

```
Switch(config)# ip access-list standard ipFlow
```

```
Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
```

```
Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255
```

1.22 permit | deny(ipv6 extended)

命令: [no] {deny | permit} icmp {{<slPv6Prefix/sPrefixlen>} | any-source | {host-source <slPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>][time-range<time-range-name>]

[no] {deny | permit} tcp { <slPv6Prefix/sPrefixlen> | any-source | {host-source <slPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

[no] {deny | permit} udp { <slPv6Prefix/sPrefixlen> | any-source | {host-source <slPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

[no] {deny | permit} <next-header> {<slPv6Prefix/sPrefixlen> | any-source | {host-source <slPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>][time-range<time-range-name>]

[no] {deny | permit} {<slPv6Prefix/sPrefixlen> | any-source | {host-source <slPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

功能: 创建一条匹配特定 IPv6 协议或所有 IPv6 协议的 IPv6 命名扩展访问规则。

参数: <slPv6Addr> 为源 IPv6 地址; <sPrefixlen> 为源 IPv6 地址的前缀长度, 范围

为 1~128； **<dIPv6Addr>** 为目的 IPv6 地址； **<dPrefixlen>** 为目的 IPv6 地址的前缀长度，范围为 1~128； **<icmp-type>**， icmp 的类型； **<icmp-code>**， icmp 的协议编号； **<dscp>**， IPv6 优先级，范围为 0~63； **<fl>**， 流标签值，范围为 0~1048575； **syn**， **ack**， **urg**， **rst**， **fin**， **psh**， tcp 标志位； **<sPort>**， 源端口号，范围为 0~65535； **<sPortMin>**， 源端口范围下边界； **<sPortMax>**， 源端口范围上边界； **<dPort>**， 目的端口号，范围为 0~65535； **<dPortMin>**， 目的端口范围下边界； **<dPortMax>**， 目的端口范围上边界； **<next-header>**， IPv6 下一头，范围为 0~255； **<time-range-name>**， 时间范围名称。

命令模式： IPv6 命名扩展访问列表配置模式

缺省情况： 没有配置任何的访问列表。

使用指南： 无。

举例： 创建名为 udpFlow 的扩展访问列表。拒绝 icmp 报文通过，允许目的地址为 2001:1:2:3::1 目的端口为 32 的 udp 包通过。

```
Switch(config)#ipv6 access-list extended udpFlow
```

```
Switch(Config-Ext-Nacl-udpFlow)# deny icmp any-source any-destination
```

```
Switch(Config-Ext-Nacl-udpFlow)# permit udp any-source host-destination 2001:1:2:3::1 d-Port 32
```

1.23 permit | deny(ipv6 standard)

命令： [no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}}

功能： 创建一条 IPv6 命名标准访问规则（rule）；本命令的 no 操作为删除此 IPv6 命名标准访问规则（rule）。

参数： **<sIPv6Prefix>**为源 IPv6 地址前缀，**<sPrefixlen>**为源 IPv6 地址前缀长度，取值范围为 1~128。**<sIPv6Addr>**为源 IPv6 地址。

命令模式： IPv6 命名标准访问列表配置模式

缺省情况： 没有配置任何的访问列表。

使用指南：

举例： 允许源地址为 2001:1:2:3::1/64 的数据包通过，拒绝其余源地址为 2001:1:2:3::1/48 的数据包通过。

```
Switch(config)# ipv6 access-list standard ipv6Flow
```

```
Switch(Config-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
```

```
Switch(Config-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48
```

1.24 permit | deny(mac extended)

命令：

```
[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }{ <smac>
<smac-mask> }} {any-destination-mac|{host-destination-mac
<host_dmac> }{ <dmac> <dmac-mask> }} [cos <cos-val>
[ <cos-bitmask> ][vlanid <vid-value> [ <vid-mask> ][ethertype <protocol>
```

```
[ <protocol-mask> ]]]
```

```
[no]{deny|permit} {any-source-mac}{host-source-mac <host_smac> }{{ <smac>
<smac-mask>          }}          {any-destination-mac}{host-destination-mac
<host_dmac>   }{{ <dmac>   <dmac-mask>   }} [ethertype <protocol>
[ <protocol-mask> ]]
```

```
[no]{deny|permit} {any-source-mac}{host-source-mac <host_smac> }{{ <smac>
<smac-mask>          }}          {any-destination-mac}{host-destination-mac
<host_dmac>   }{{ <dmac>   <dmac-mask>   }} [vlanid <vid-value>
[ <vid-mask> ]][ethertype <protocol> [ <protocol-mask> ]]]
```

```
[no]{deny|permit} {any-source-mac}{host-source-mac <host_smac> }{{ <smac>
<smac-mask>          }}          {any-destination-mac}{host-destination-mac
<host_dmac> }{{ <dmac> <dmac-mask> }} [untagged-eth2 [ethertype <protocol>
[protocol-mask]]]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac <host_smac> }{{ <smac>
<smac-mask>          }}          {any-destination-mac}{host-destination-mac
<host_dmac> }{{ <dmac> <dmac-mask> }} [untagged-802-3]
```

```
[no]{deny|permit} {any-source-mac}{host-source-mac <host_smac> }{{ <smac>
<smac-mask>          }}          {any-destination-mac}{host-destination-mac
<host_dmac> }{{ <dmac> <dmac-mask> }} [tagged-eth2 [cos <cos-val>
[ <cos-bitmask> ]] [vlanid <vid-value> [ <vid-mask> ]] [ethertype <protocol>
[ <protocol-mask> ]]]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac <host_smac> }{{ <smac>
<smac-mask>          }}          {any-destination-mac}{host-destination-mac
<host_dmac> }{{ <dmac> <dmac-mask> }} [tagged-802-3 [cos <cos-val>
[ <cos-bitmask> ]] [vlanid <vid-value> [ <vid-mask> ]]]
```

功能：定义一条扩展命名 MAC ACL 规则，No 命令删除一个扩展命名 MAC ACL 访问表规则。

参数：any-source-mac: 任何源 MAC 地址；any-destination-mac: 任何目的 MAC 地址；host_smac , smac: 源 MAC 地址；smac-mask 源 MAC 地址的掩码(反掩码)；host_dmac , dmac 目的 MAC 地址；dmac-mask 目的 MAC 地址的掩码(反掩码)；untagged-eth2: 未标记的 ethernet II 包格式；tagged-eth2: 标记的 ethernet II 包格式；untagged-802-3: 未标记的 ethernet 802.3 包格式；tagged-802-3: 标记的 ethernet 802.3 包格式；cos-val: cos 值，0-7；cos-bitmask: cos 掩码，0-7 反掩码且掩码比特连续；vid-value: vlan 号，1-4094；vid-bitmask: vlan 掩码，0-4095，反掩码且掩码比特连续；

protocol: 特定的以太网协议号, 1536—65535; **protocol-bitmask:** 协议掩码, 0—65535, 反掩码且掩码比特连续

注意: 掩码比特连续是指, 掩码有效位必须从左第一位开始连续有效, 不允许中间插入无效位, 例如: 一个字节的反掩码形式为: 00001111b ; 正掩码形式为: 11110000; 不允许 00010011。

命令模式: 命名扩展 MAC 访问列表配置模式

缺省配置: 没有配置任何的访问列表

使用指南:

举例: 不允许转发源MAC地址是00-12-11-23-XX-XX的802.3的数据报文。

```
Switch(config)# mac-access-list extended macExt
```

```
Switch(Config-Mac-Ext-Nacl-macExt)# deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac untagged-802-3
```

```
Switch(Config-Mac-Ext-Nacl-macExt)# deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any tagged-802
```

1.25 permit | deny(mac-ip extended)

命令:

```
[no] {deny|permit}
```

```
{any-source-mac[{host-source-mac<host_smac>}]<smac><smac-mask>}}
{any-destination-mac[{host-destination-mac<host_dmac>}]<dmac><dmac-mask>}}
icmp[{<source><source-wildcard>}]any-source[{host-source<source-host-ip>}]
[{<destination><destination-wildcard>}]any-destination[{host-destination
<destination-host-ip>}] [<icmp-type> [<icmp-code>]] [precedence <precedence>]
[tos <tos>][time-range<time-range-name>]
```

```
[no]{deny|permit}
```

```
{any-source-mac[{host-source-mac<host_smac>}]<smac><smac-mask>}}
{any-destination-mac[{host-destination-mac<host_dmac>}]<dmac><dmac-mask>}}
igmp[{<source><source-wildcard>}]any-source| {host-source<source-host-ip>}}
[{<destination><destination-wildcard>}]any-destination|{host-destination
<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]
```

```
[no]{deny|permit}{any-source-mac[{host-source-mac <host_smac> }] { <smac>
<smac-mask>
}}{any-destination-mac[{host-destination-mac
<host_dmac> }] { <dmac> <dmac-mask> }}tcp[{ <source>
<source-wildcard> }]any-source| {host-source <source-host-ip> }}[s-port { <port1> |
range <sPortMin> <sPortMax> }] {{ <destination> <destination-wildcard> } |
any-destination| {host-destination <destination-host-ip> }} [d-port { <port3> | range
<dPortMin> <dPortMax> }] [ack + fin + psh + rst + urg + syn] [precedence
<precedence> ] [tos <tos> ] [time-range<time-range-name>]
```

```
[no]{deny|permit}{any-source-mac[{host-source-mac <host_smac> }] { <smac>
```

```
<smac-mask> }}{any-destination-mac}{host-destination-mac <host_dmac> }|
{ <dmac> <dmac-mask> }}udp{{ <source> <source-wildcard> }}any-source|
{host-source <source-host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> }}any-destination| {host-destination
<destination-host-ip> }} [d-port { <port3> | range <dPortMin> <dPortMax> }]
[precedence <precedence> ] [tos <tos> ] [time-range<time-range-name>]
```

```
[no]{deny|permit}{any-source-mac}{host-source-mac<host_smac>}{<smac>
<smac-mask>}}{any-destination-mac}{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}}{eigrp|gre|igrp|ip|ipinip|ospf}{<protocol-num>}}
{{<source><source-wildcard>}}any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}}any-destination|{host-destination
<destination-host-ip>}} [precedence <precedence>] [tos
<tos>][time-range<time-range-name>]
```

功能：定义一条扩展命名 MAC-IP ACL 规则，No 命令删除一个扩展数字 MAC-IP ACL 访问表规则。

参数：num 访问表号。这是一个从 3100—3199 的十进制号；**deny** 如果规则匹配，拒绝访问；**permit** 如果规则匹配，允许访问；**any-source-mac**：任何源 MAC 地址；**any-destination-mac**：任何目的 MAC 地址；**host_smac**，**smac**：源 MAC 地址；**smac-mask**：源 MAC 地址的掩码(反掩码)；**host_dmac**，**dmac** 目的 MAC 地址；**dmac-mask** 目的 MAC 地址的掩码(反掩码)；**protocol** 名字或 IP 协议的号。它可以是关键字 eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, 也可以是表 IP 协议号的 0 到 255 的一个整数。为了匹配任何 Internet 协议（包括 ICMP，TCP 和 UDP）使用关键字 ip；**source-host-ip**, **source** 包发送的源网络或源主机号。32 位二进制数，点分十进制表示；**host-source**:表示地址是源主机 IP 地址，否则是网络 IP 地址；**source-wildcard**:源 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**destination-host-ip**, **destination** 包发送时要去往的目的网络或主机号。32 位二进制数，点分十进制表示；**host-source**:表示地址是目的主机 IP 地址，否则是网络 IP 地址；**destination-wildcard**:目的 IP 的掩码。用四个点隔开的十进制数表示的 32 位二进制数，反掩码；**s-port** (可选): 表示要匹配 TCP/UDP 源端口；**port1** (可选): TCP/UDP 源端口号值，端口号是一个 0 到 65535 的数字；**<sPortMin>**，源端口范围下边界；**<sPortMax>**，源端口范围上边界；**d-port** (可选): 表示要匹配 TCP/UDP 目的端口；**port3** (可选): TCP/UDP 目的端口号值，端口号是一个 0 到 65535 的数字；**<dPortMin>**，目的端口范围下边界；**<dPortMax>**，目的端口范围上边界；**[ack] [fin] [psh] [rst] [urg] [syn]** (可选) 只对 TCP 协议，可选多个标志位，当 TCP 数据报[ack] [fin] [psh] [rst] [urg] [syn]的相应位设置时，即初始化 TCP 数据报以形成一个连接时出现匹配；**precedence** (可选) 包可由优先级过滤，为 0 到 7 的数字；**tos** (可选)包可由服务级类型过滤，为 0 到 15 的数字；**icmp-type** (可选) ICMP 包可由 ICMP 报文类型过滤。类型是数字 0 到 255；**icmp-code** (可选) ICMP 包可由 ICMP 报文码过滤。该代码是数字 0 到 255；**igmp-type** (可选) IGMP 包可由 IGMP 报文类型或报文明过滤。类型是数字 0 到 15；**<time-range-name>**，时间范围名称。

命令模式：命名扩展 MAC-IP 访问列表配置模式

缺省情况：没有配置任何的访问列表。

使用指南：无。

举例：拒绝任意源 MAC 地址及目的 MAC 地址，任意源 IP 地址及目的 IP 地址，且源端口

是 100，目的端口是 40000 的 UDP 报文通过

```
Switch(config)# mac-ip-access-list extended macIpExt
```

```
Switch(Config-MacIp-Ext-Nacl-macIpExt)# deny any-source-mac any-destination-mac
udp any-source s-port 100 any-destination d-port 40000
```

1.26 show access-lists

命令： show access-lists [**<num>** | **<acl-name>**]

功能： 显示配置的访问控制列表。

参数： **<acl-name>**，特定的访问控制列表命名字符串；**<num>**，特定的访问控制列表的编号。

缺省情况： 无。

命令模式： 特权和配置模式

使用指南： 不指定访问控制列表的名字时，会显示所有的访问控制列表；used x time (s) 表明了此 ACL 被引用的次数。

举例：

```
Switch#show access-lists
```

```
access-list 10(used 0 time(s))
```

```
access-list 10 deny any-source
```

```
access-list 100(used 1 time(s))
```

```
access-list 100 deny ip any-source any-destination
```

```
access-list 100 deny tcp any-source any-destination
```

```
access-list 1100(used 0 time(s))
```

```
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800
```

```
access-list 3100(used 0 time(s))
```

```
access-list 3100 deny any-source-mac any-destination-mac udp any-source s-port
100 any-destination d-port 40000
```

显示内容	解释
access-list 10(used 1 time(s))	数字 ACL10，被引用 0 次
access-list 10 deny any-source	拒绝所有 IP 数据包通过
access-list 100(used 1 time(s))	数字 ACL100，被引用 1 次
access-list 100 deny ip any-source any-destination	拒绝任意源 IP 地址及目的 IP 地址的 IP 包通过
access-list 100 deny tcp any-source any-destination	拒绝任意源 IP 地址及目的 IP 地址的 TCP 包通过
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	允许任意源 MAC 地址任意目的 MAC 地址的 tagged-eth2，且其第 15 16 个字节分别为 0x08，0x0 的包通过
access-list 3100 permit any-source-mac	拒绝任意源 MAC 地址及目的 MAC 地址，任

any-destination-mac udp any-source s-port 100 any-destination d-port 40000	意源 IP 地址及目的 IP 地址，且源端口是 100，目的端口是 40000 的 UDP 报文通过
--	--

1.27 show access-group

命令： show access-group in (interface {Ethernet | Ethernet IFNAME})

功能： 显示端口上 ACL 绑定情况。

参数： IFNAME，端口名。

缺省情况： 无。

命令模式： 特权和配置模式。

使用指南： 不指定接口名时，会显示所有端口上绑定的 ACL。

举例：

Switch#show access-group

interface name:Ethernet1/1

IP Ingress access-list used is 100, traffic-statistics Disable.

interface name:Ethernet1/2

IP Ingress access-list used is 1, packet(s) number is 11110.

显示内容	解释
interface name:Ethernet1/1	端口 Ethernet1/1 的绑定情况
IP Ingress access-list used is 100	端口 Ethernet1/1 入口方向绑定了编号 100 的数字扩展 ACL
packet(s) number is 11110	统计到匹配此 ACL 规则的数据包数

1.28 show acl vlan-division <vlan-id> to <vlan-id>

本交换机不支持该命令。

1.29 show firewall

命令： show firewall

功能： 显示包过滤功能配置信息。

参数： 无。

缺省情况： 无。

命令模式： 特权和配置模式。

使用指南： 无。

举例：

Switch#show firewall

Firewall Status: Enable.

Firewall Default Rule: Permit.

显示内容	解释
Firewall Status: Enable	包过滤功能打开
Firewall Default Rule: Permit	包过滤默认动作为 permit

1.30 show ipv6 access-lists

命令： **show ipv6 access-lists** [**<num>**]**<acl-name>**

功能： 显示配置的 IPv6 访问控制列表。

参数： <num>为特定的访问控制列表的编号，取值范围为 500～699，其中 500～599 为数字标准 IPv6 ACL 编号，600～699 为数字扩展 IPv6 ACL 编号；<acl-name>为特定的访问控制列表命名字符串，长度为 1～16。

缺省情况： 无。

命令模式： 特权和配置模式。

使用指南： 不指定访问控制列表的名字时，会显示所有的访问控制列表；used x time（s）表明了此 ACL 被引用的次数。

举例：

```
Switch #show ipv6 access-lists
```

```
ipv6 access-list 500(used 1 time(s))
```

```
    ipv6 access-list 500 deny any-source
```

```
ipv6 access-list 510(used 1 time(s))
```

```
    ipv6 access-list 510 deny ip any-source any-destination
```

```
    ipv6 access-list 510 deny tcp any-source any-destination
```

```
ipv6 access-list 520(used 1 time(s))
```

```
    ipv6 access-list 520 permit ip any-source any-destination
```

1.31 show time-range

命令： **show time-range**<word>

功能： 显示时间范围功能配置信息。

参数： **word** 指定要显示的 time-range 的名字

缺省情况： 无。

命令模式： 特权和配置模式。

使用指南： 不指定 time-range 的名字时，显示所有的 time-range。

举例：

```
Switch#show time-range
```

```
time-range timer1 (inactive, used 0 times)
```

```
    absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
```

```
time-range timer2 (inactive, used 0 times)
```

```
    absolute-periodic Monday 0:0:0 to Friday 23:59:59
```

1.32 time-range

命令： [no] time-range <time_range_name>

功能： 创建一个名为 time_range_name 的时间范围名，并同时进入时间范围模式。

参数： time_range_name 时间范围名字，必须用字母字符开头，名字最大长度为 16 个字符。

命令模式： 全局配置模式

缺省情况： 没有时间范围配置。

使用指南： 无。

举例： 创建一个名为 admin_timer 的时间范围。

Switch(config)#time-range admin_timer

第 2 章 自定义 ACL 命令

2.1 permit | deny

命令: {permit | deny} [packet-type {ipv4 | ipv6 | l2-eth2 | l2-llc | l2-snap | mpls}]
[window1 <value> <mask>] [window2 <value> <mask>] [window3 <value> <mask>]
[window4 <value> <mask>] [window5 <value> <mask>] [window6 <value> <mask>]
[window7 <value> <mask>] [window8 <value> <mask>] [window9 <value> <mask>]
[window10 <value> <mask>] [window11 <value> <mask>] [window12 <value>
<mask>] [window13 <value> <mask>] [window14 <value> <mask>] [window15
<value> <mask>] [window16 <value> <mask>]

[no] { permit | deny } [packet-type {ipv4 | ipv6 | l2-eth2 | l2-llc | l2-snap | mpls}]
[window1 <value> <mask>] [window2 <value> <mask>] [window3 <value> <mask>]
[window4 <value> <mask>] [window5 <value> <mask>] [window6 <value> <mask>]
[window7 <value> <mask>] [window8 <value> <mask>] [window9 <value> <mask>]
[window10 <value> <mask>] [window11 <value> <mask>] [window12 <value>
<mask>] [window13 <value> <mask>] [window14 <value> <mask>] [window15
<value> <mask>] [window16 <value> <mask>]

功能: 在命名自定义 acl 访问列表中增加一条规则 (rule) 表项; 本命令的 no 操作为删除一条自定义访问列表。

参数: deny 如果规则匹配, 拒绝访问; permit 如果规则匹配, 允许访问; packet-type 的各个类型是针对不同的报文类型匹配; 各个 window 的 <value> 和 <mask> 为一个 2 字节长度 16 进制数。

命令模式: 命名自定义访问列表模式

缺省情况: 没有配置任何的规则

使用指南: 当用户第一次指定特定 <name> 时, 创建此编号的 ACL, 之后在此 ACL 中添加表项。

举例: 配置名为 aclName_test 的自定义 acl, 允许报文的前两个字节为 0x4501 的包通过。

```
Switch(config)#userdefined-access-list standard offset window1 0
```

```
Switch(config)#userdefined-access-list standard aclName_test
```

```
Switch(config-udf-std-nacl-aclname_test)# permit window1 4501 FFFF
```

2.2 udf-access-list standard

命令: udf-access-list standard <name>

no udf-access-list standard <name>

功能: 创建一条命名自定义访问列表; 本命令的 no 操作为删除该自定义访问列表。

参数: <name> 为访问列表名, 字符串长度为 1-64, 不允许为纯数字序列

命令模式: 全局配置模式

缺省情况: 没有配置任何的访问列表

使用指南: 创建一条命名自定义访问列表, 并进入命名自定义访问列表配置模式。

举例：创建一个名为 acl1 的自定义访问列表。

```
Switch(config)# udf-access-list standard acl1
```

2.3 userdefined-access-list standard offset

命令： userdefined-access-list standard offset [window1 <offset>] [window2 <offset>] [window3 <offset>] [window4 <offset>] [window5 <offset>] [window6 <offset>] [window7 <offset>] [window8 <offset>] [window9 <offset>] [window10 <offset>] [window11 <offset>] [window12 <offset>] [window13 <offset>] [window14 <offset>] [window15 <offset>] [window16 <offset>]

no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12] [window13] [window14] [window15] [window16]

功能：创建标准自定义访问列表模板，如果已有此模板则修改模板对应的 window；本命令的 no 操作为删除标准自定义访问列表模板对应 window，如果未指定任何 window 则删除整个标准自定义访问列表模板。

参数：

window1-window16 自定义窗口 1 至 16

offset 配置的偏移量<0-31>（单位为 2 字节）

命令模式：全局配置模式

缺省情况：没有配置模板

使用指南：<offset>为配置一个 window 的偏移量，取值范围为<0-31>，单位为 2Bytes，即 0 代表偏移 0Bytes，1 代表偏移 2Bytes，可以配置至多 16 个 window 的偏移起始位置和偏移量。全局共享一个基本自定义 ACL 模板，在配置有使用了某个 window 的自定义 ACL 规则时该模板中对应的 window 无法被修改，当没有规则引用某个 window 时可以用本命令修改这个 window 的配置。

删除模板命令可以删除模板中的某个或某些窗口的偏移配置或删除整个模板的配置（未指定任何具体的 window）。必须当模板对应 window 没有被自定义 ACL 规则使用时才能删除成功。

举例：创建全局模板，使用 7 个 window（3-9），分别配置偏移起始位和偏移量：

```
Switch(config)#userdefined-access-list standard offset window3 l2 0 window4 l2 2  
window5 l3 0 window6 l3 1 window7 l3 2 window8 l4 1 window9 l4 2
```

2.4 userdefined-access-list extended offset

本交换机不支持此命令。

2.5 userdefined-access-list standard

命令： userdefined-access-list standard <num> {deny | permit} [packet-type {ipv4 | ipv6 | l2-eth2 | l2-llc | l2-snap | mpls}] [window1 <value> <mask>] [window2 <value> <mask>] [window3 <value> <mask>] [window4 <value> <mask>] [window5 <value>

```
<mask>] [window6 <value> <mask>] [window7 <value> <mask>] [window8 <value>
<mask>] [window9 <value> <mask>] [window10 <value> <mask>] [window11
<value> <mask>] [window12 <value> <mask>] [window13 <value> <mask>]
[window14 <value> <mask>] [window15 <value> <mask>] [window16 <value>
<mask>]
```

no userdefined-access-list <num>

功能：创建一条数字标准自定义访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的 no 操作为删除一条标准自定义访问列表。

参数：<num>访问表号，这是一个从 1200—1299 的十进制号；deny 如果规则匹配，拒绝访问；permit 如果规则匹配，允许访问；packet-type 的各个类型是针对不同的报文类型匹配；各个 window 的<value>和<mask>为一个 2 字节长度 16 进制数。

命令模式：全局配置模式

缺省情况：没有配置任何的访问列表

使用指南：当用户第一次指定特定<num>时，创建此编号的 ACL，之后在此 ACL 中添加表项。

举例：允许报文的前两个字节为 0x4501 的包通过。

```
Switch(config)#userdefined-access-list standard offset window1 0
```

```
Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF
```

2.6 userdefined-access-list extended

本交换机不支持此命令。

2.7 userdefined access-group

命令：userdefined access-group {<name>|<num>} {in} [traffic-statistic]

no userdefined access-group {<name>|<num>} {in}

功能：在端口的某个方向上应用一条 userdefined-access-list，并且根据可选项决定是否对 ACL 规则加上统计计数器；本命令的 no 操作为删除绑定在端口上的 userdefined-access-list。

参数：<num>访问表的名字，这是一个从 1200-1299 的十进制号数字名字；

<name>访问表的名字，字符串长度为 1-64，不允许为纯数字序列。

命令模式：物理端口配置模式

缺省情况：端口没有绑定 userdefined-access-list

使用指南：一个端口可以在入口方向上绑定一个自定义访问列表，自定义访问列表与其它类型的访问列表可以同时配置在同一个端口入方向上，不同类型的访问列表同时匹配时遵循 deny 优先原则，即如果有某类访问列表匹配 deny 规则则一定会执行 deny，反之会 permit 报文。

举例：已配置的自定义访问列表如下：

```
Switch(config)#userdefined-access-list standard offset window1 0
```

```
Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF
```

绑定自定义访问列表至端口 Ethernet1/1：

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

Switch(config-if-ethernet1/1)#userdefined access-group 1200 in

2.8 vac1 userdefined access-group

本交换机不支持此命令。

第 3 章 802.1x 配置命令

注:目前仅 7.5 版本支持 802.1x 功能。

3.1 authentication dot1x radius none

本交换机不支持此命令。

3.2 debug dot1x detail

命令: **debug dot1x detail {pkt-send | pkt-receive | internal| all | userbased | webbased} interface [ethernet] <interface-name>**

no debug dot1x detail {pkt-send | pkt-receive | internal | all | userbased | webbased} interface [ethernet] <interface-name>

功能: 打开 dot1x 的细节调试信息; 本命令的 no 操作为关闭 dot1x 的细节调试信息。

参数: **pkt-send:** 打开 dot1x 的发送包调试信息;
pkt-receive: 打开 dot1x 的接收包调试信息;
internal: 打开 dot1x 的内部细节调试信息;
all: 打开 dot1x 的所有以上细节调试信息;
userbased: 基于用户认证方式;
webbased: 基于 Web 认证方式;
<interface-name>: 端口名称。

命令模式: 特权配置模式。

使用指南: 打开 dot1x 细节调试信息, 可以查看 dot1x 协议运行的细节过程, 在遇到故障时有助于监测故障原因。

举例: 打开端口 1/1 下 dot1x 的所有细节调试信息。

Switch#debug dot1x detail all interface ethernet 1/1

3.3 debug dot1x error

命令: **debug dot1x error**
no debug dot1x error

功能: 打开 dot1x 的出错调试信息; 本命令的 no 操作为关闭 dot1x 的出错调试信息。

参数: 无。

命令模式: 特权配置模式。

使用指南: 打开 dot1x 出错调试信息, 可以查看 dot1x 协议运行过程中的出错信息, 在遇到故障时有助于监测故障原因。

举例: 打开 dot1x 出错调试信息。

Switch#debug dot1x error

3.4 debug dot1x fsm

命令: **debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>**
no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <interface-name>

功能: 打开 dot1x 的状态机调试信息; 本命令的 no 操作为关闭 dot1x 的状态机调试信息。

命令模式: 特权配置模式。

参数: **all**: 打开 dot1x 的所有状态机调试信息;

aksm: 打开 Authenticator Key Transmit 状态机调试信息;

asm: 打开 Authenticator 状态机调试信息;

basm: 打开 Backend Authentication 状态机调试信息;

ratsm: 打开 Re-Authentication Timer 状态机调试信息;

<interface-name>: 端口名称。

使用指南: 打开 dot1x 调试信息, 可以查看 dot1x 协议的协商过程, 在遇到故障时有助于监测故障原因。

举例: 打开 dot1x 状态机调试信息。

Switch#debug dot1x fsm asm interface ethernet1/1

3.5 debug dot1x packet

命令: **debug dot1x packet {all | receive | send} interface <interface-name>**
no debug dot1x packet {all | receive | send} interface <interface-name>

功能: 打开 dot1x 的报文调试信息; 本命令的 no 操作为关闭 dot1x 的报文调试信息。

命令模式: 特权配置模式。

参数: **send**: 打开 dot1x 的发包调试信息;

receive: 打开 dot1x 的收包调试信息;

all: 打开 dot1x 的收包和发包调试信息;

<interface-name>: 端口名称。

使用指南: 打开 dot1x 调试信息, 可以查看 dot1x 协议的协商过程, 在遇到故障时有助于监测故障原因。

举例: 打开 dot1x 报文调试信息。

Switch#debug dot1x packet all interface ethernet1/1

3.6 dot1x accept-mac

命令: **dot1x accept-mac <mac-address> [interface <interface-name>]**
no dot1x accept-mac <mac-address> [interface <interface-name>]

功能: 向 dot1x 地址过滤表中添加一个 MAC 地址表项, 如果指定端口则添加的表项仅适用于指定端口, 不指定端口则添加的表项适用于全部端口; 本命令的 no 操作为删除 dot1x 的地址过滤表中的表项。

参数: **<mac-address>**为 MAC 地址; **<interface-name>**为接口名称及接口号。

命令模式: 全局配置模式。

缺省情况：无。

使用指南：交换机的 dot1x 地址过滤功能是根据 MAC 地址过滤表实现的，dot1x 地址过滤表由用户手工添加或删除。当添加 dot1x 地址过滤表项时指定了端口，则该地址过滤表项仅适用于该端口；若添加时未指定端口，则该地址过滤表项适用于交换机所有端口。当交换机的 dot1x 地址过滤功能打开，交换机会对认证者的 MAC 地址进行过滤，只有在 dot1x 地址过滤表中存在的客户发起的认证请求才能被接受，否则将被拒绝。

举例：将 MAC 地址 00-01-34-34-2e-0a 添加到 Ethernet 1/5 的过滤表中。

Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/5

3.7 dot1x eapor enable

命令：dot1x eapor enable

no dot1x eapor enable

功能：设置交换机采用 EAP 中继的方式进行认证；本命令的 no 操作为设置交换机采用 EAP 本地终结的方式进行认证。

命令模式：全局配置模式

缺省情况：交换机采用 EAP 中继的方式进行认证。

使用指南：交换机与 Radius 认证服务器之间可能采用以太网方式连接或者采用 PPP 方式连接。如果交换机与 Radius 认证服务器之间采用以太网连接，那么交换机需要采用 EAP 中继的方式进行认证（即 EAPoR 认证）；如果交换机与 Radius 认证服务器之间采用 PPP 方式连接，则交换机需要采用 EAP 本地终结的方式进行认证（即 CHAP 认证）。根据交换机与认证服务器的连接方式的不同，交换机应该采用不同的认证方式进行认证。

举例：设置交换机采用 EAP 本地终结的方式进行认证。

Switch(config)#no dot1x eapor enable

3.8 dot1x enable

命令：dot1x enable [vlan-pool WORD]

no dot1x enable [vlan-pool WORD]

功能：打开交换机全局及端口的 802.1x 功能；本命令的 no 操作为关闭 802.1x 功能。

参数：WORD：指定 vlan 池列表。

命令模式：全局配置模式及端口配置模式

缺省情况：交换机在全局下不打开 802.1x 功能；若交换机在全局下打开 802.1x 功能，则端口缺省也不打开 802.1x 功能。

使用指南：如果要对端口进行 802.1x 认证时，首先要打开全局下的 802.1x 功能，再在相应的端口下打开 802.1x 功能。对于只在端口下的某些 VLAN 或某个 VLAN 开启 802.1x 功能的情况，则只需要打开端口 vlan 下的 802.1 功能。如果该端口已经打开了 Spanning Tree，或者使能了 mac 绑定，或者是 Trunk 端口、端口聚合组的成员，则必须关闭端口下的 Spanning Tree 功能、或者关闭 mac 绑定、或者改变端口为 Access 端口、取消参加端口汇聚组，否则无法打开端口下的 802.1x 功能。

举例：启动交换机的 802.1x 功能，新建 vlan-pool 1（包含 vlan id 2）；并且打开 1/12 号端口下 vlan 2 的 802.1x 功能。

Switch(config)#dot1x enable

```
Switch(config)#vlan-pool 1 2
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable vlan-pool 1
```

3.9 dot1x dhcp passthrough

命令： dot1x dhcp passthrough
no dot1x dhcp passthrough

功能： 打开交换机端口的 dhcp 透传功能，允许终端用户在未认证前通过 dhcp 获取地址；本命令的 no 操作为关闭该功能。

命令模式： 端口配置模式。

缺省情况： 交换机不打开 dhcp 透传功能。

使用指南： 在打开该功能时，首先要打开全局和端口下的 802.1x 功能，否则不能打开 dhcp 透传功能。打开该功能后，用户不需要通过认证，也可通过 dhcp 获取地址。

举例： 在 Ethernet1/12 端口上开启 dhcp 透传功能。

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable
Switch(Config-If-Ethernet1/12)#dot1x dhcp passthrough
```

3.10 dot1x guest-vlan

命令： dot1x guest-vlan <vlanid>
no dot1x guest-vlan

功能： 设置指定端口的 guest-vlan；本命令的 no 操作为删除 guest-vlan。

参数： <vlanid> 所配置的 Vlan id，取值范围为 1-4094。

命令模式： 端口配置模式。

缺省情况： 端口上不配置 802.1x guest-vlan 功能。

使用指南： 如果因为没有专用的认证客户端或者客户端版本过低等原因，导致在一定的时间内端口上无客户端认证成功，接入设备会把该端口加入到 Guest VLAN。用户在 Guest VLAN 中可以获取 802.1x 客户端软件，升级客户端，或执行其他一些应用升级程序（例如防病毒软件、操作系统补丁程序等）。当 Guest VLAN 中端口下的用户发起认证，如果认证失败，该端口将会仍然处在 Guest VLAN 内；如果认证成功，分为以下两种情况：

- ✎ 认证服务器下发一个 Auto VLAN，这时端口离开 Guest VLAN，加入下发的 Auto VLAN 中。用户下线后，端口会被重新划分到所配置的 Guest Vlan 内。
- ✎ 认证服务器不下发 VLAN，这时端口离开 Guest VLAN，加入配置的 VLAN 中。用户下线后，端口会被重新划分到所配置的 GuestVlan 内。

注意事项：

- ✎ 不同的端口可以配置不同的 Guest VLAN，但一个端口只能配置一个 Guest VLAN。
- ✎ 当端口的接入控制方式为 portbased 时，Guest VLAN 才能生效；若端口的接入控制为 macbased 或 userbased，Guest VLAN 能够配置成功，但不生效。

举例： 设置端口 Ethernet1/3 的 Guest-Vlan 为 Vlan 10。

```
Switch(Config-If-Ethernet1/3)#dot1x guest-vlan 10
```

3.11 dot1x macfilter enable

命令：dot1x macfilter enable

no dot1x macfilter enable

功能：打开交换机的 dot1x 地址过滤功能；本命令的 no 操作为关闭 dot1x 地址过滤功能。

命令模式：全局配置模式

缺省情况：交换机关闭 dot1x 地址过滤功能。

使用指南：当打开交换机的 dot1x 地址过滤功能，交换机会对认证者的 MAC 地址进行过滤，只有在 dot1x 地址过滤表中存在的客户发起的认证请求才能被接受。

举例：打开交换机的 dot1x 地址过滤功能。

Switch(config)#dot1x macfilter enable

3.12 dot1x macbased guest-vlan

命令：dot1x macbased guest-vlan <vlanid>

no dot1x macbased guest-vlan

功能：设置指定基于 mac 认证的端口的 guest-vlan；本命令的 no 操作为删除 guest-vlan。

参数：<vlanid> 所配置的 Vlan id，取值范围为 1-4094。

命令模式：端口配置模式。

缺省情况：端口上不配置 802.1x macbased guest-vlan 功能。

使用指南：如果因为没有专用的认证客户端或者客户端版本过低等原因，导致在一定的时间内端口上无客户端认证成功，接入设备会把该用户加入到 Guest VLAN。用户在 Guest VLAN 中可以获取 802.1x 客户端软件，升级客户端，或执行其他一些应用升级程序（例如防病毒软件、操作系统补丁程序等）。当 Guest VLAN 中端口下的用户发起认证，如果认证失败，该端口将会仍然处在 Guest VLAN 内；如果认证成功，分为以下两种情况：

- 1 认证服务器下发一个 Auto VLAN，这时用户离开 Guest VLAN，加入下发的 Auto VLAN 中。用户下线后，用户会被重新划分到所配置的 Guest Vlan 内。
- 2 认证服务器不下发 VLAN，这时用户离开 Guest VLAN，加入配置的 Native VLAN 中。用户下线后，用户会被重新划分到所配置的 Guest Vlan 内。

注意事项：

- 1 只有基于 mac 认证且为 HYBRID 模式的端口才能配置 dot1x macbased guest-vlan
- 2 不同的端口可以配置不同的 macbased Guest VLAN，但一个端口只能配置一个 macbased Guest VLAN。

举例：设置端口 Ethernet1/3 的 Guest-Vlan 为 Vlan 10。

Switch(Config-If-Ethernet1/3)#dot1x macbased guest-vlan 10

3.13 dot1x macbased port-down-flush

命令：dot1x macbased port-down-flush

no dot1x macbased port-down-flush

功能：打开该命令，当基于 mac 进行 dot1x 认证的端口 down 时，删除该端口上已经认证通过的用户；本命令的 no 操作不对该情况下已认证用户进行下线操作。

命令模式：全局配置模式

缺省情况：交换机缺省未打开该命令。

使用指南：当基于mac进行认证的用户在不同端口中切换时，需要在原来已经认证上的端口上删除才能在新的端口上重新进行认证，这时需要开启该命令来保证原来端口上删除认证通过的用户。

举例：基于mac进行dot1x认证的端口down时，删除该端口上已经认证通过的用户。

Switch(config)#dot1x macbased port-down-flush

3.14 dot1x max-req

命令：dot1x max-req <count>

no dot1x max-req

功能：设置交换机在没有收到 supplicant 回应而重新启动认证前，发送 EAP-request/MD5 帧的最大次数；本命令的 no 操作为恢复缺省值。

参数：<count> 为发送 EAP-request/ MD5 帧的次数，取值范围为 1~10。

命令模式：全局配置模式

缺省情况：最大次数为 2 次。

使用指南：用户在配置发送 EAP-request/ MD5 帧的最大次数时，建议使用缺省值。

举例：更改发送 EAP-request/ MD5 帧的最大次数为 5 次。

Switch(config)#dot1x max-req 5

3.15 dot1x user allow-movement

命令：dot1x user allow-movement

no dot1x user allow-movement

功能：打开交换机允许用户迁移端口认证功能；本命令的 no 操作为关闭用户迁移端口认证功能。

命令模式：全局配置模式

缺省情况：交换机关闭用户迁移端口认证功能。

使用指南：当打开交换机允许用户迁移端口认证功能，交换机允许用户迁移端口认证。一个典型的应用是在交换机下接 hub 的情况下，用户由 hub 迁移到交换机其他端口认证，此时可以打开此命令。

举例：打开用户迁移端口认证功能。

Switch(config)#dot1x user allow-movement

3.16 free-resource destination

命令：free-resource destination {ipv4 | ipv6} <prefix>/<mask>

no free-resource destination [ipv4 | ipv6] <prefix>/<mask>

功能：设置交换机全局的 ipv4 或 ipv6 有限资源；本命令的 no 操作为删除指定有限资源。

参数：<prefix> 为有限资源所在的网段，ipv4 地址为点分十进制格式，ipv6 地址为冒号分的十六进制格式；

<mask> 为有限资源所在的网络掩码位数。

命令模式： 全局配置模式。

缺省情况： 交换机没有缺省的有限资源。

使用指南： 配置了有限资源后，没有经过 802.1x 认证的用户能够访问本命令配置的有限资源。

举例： 设置有限资源所在的网段为 100.1.1.0，网络掩码为 255.255.255.0。

Switch (config): free-resource destination ipv4 100.1.1.0/24

3.17 dot1x max-user macbased

本交换机不支持此命令。

3.18 dot1x max-user userbased

本交换机不支持此命令。

3.19 dot1x portbased mode single-mode

本交换机不支持此命令。

3.20 dot1x port-control

本交换机不支持此命令。

3.21 dot1x port-method

本交换机不支持此命令。

3.22 dot1x privateclient enable

本交换机不支持此命令。

3.23 dot1x privateclient protect enable

本交换机不支持此命令。

3.24 dot1x re-authenticate

命令： dot1x re-authenticate [interface <interface-name>]

功能：设置即时对所有端口或某个指定端口进行 802.1x 重认证，不必等待超时。

参数：<interface-name>为端口号，如果无参数则表示所有端口。

命令模式：全局配置模式

使用指南：本命令为全局模式下的命令，当配置本命令后，交换机立刻对客户端进行重认证，不需要等待重新认证定时器超时。认证之后，该命令就无效了。

举例：对端口 Ethernet 1/8 进行即时重认证。

Switch(config)#dot1x re-authenticate interface ethernet 1/8

3.25 dot1x re-authentication

命令：dot1x re-authentication

no dot1x re-authentication

功能：设置允许对 supplicant 进行周期性重认证；本命令的 no 操作为关闭该功能。

命令模式：全局配置模式

缺省情况：缺省情况下周期性重认证功能是关闭的。

使用指南：当打开对 supplicant 的周期性重认证功能，交换机会周期性的对 supplicant 进行重新认证。一般情况下建议不打开周期性重认证功能。

举例：打开对认证者进行周期性重认证功能。

Switch(config)#dot1x re-authentication

3.26 dot1x timeout quiet-period

命令：dot1x timeout quiet-period <seconds>

no dot1x timeout quiet-period

功能：设置 supplicant 在认证失败后端口保持静默状态的时间；本命令的 no 操作为恢复缺省值。

参数：<seconds>为端口保持静默状态的时间长度值，单位为秒，取值范围为 1~65535。

命令模式：全局配置模式

缺省情况：缺省为 10 秒。

使用指南：建议使用缺省值。

举例：设置静默时间为 120 秒。

Switch(config)#dot1x timeout quiet-period 120

3.27 dot1x timeout re-authperiod

命令：dot1x timeout re-authperiod <seconds>

no dot1x timeout re-authperiod

功能：设置交换机对 supplicant 重认证的时间间隔；本命令的 no 操作为恢复缺省值。

参数：<seconds>重认证的时间间隔，单位为秒，取值范围为 1~65535。

命令模式：全局配置模式。

缺省情况：缺省为 3600 秒。

使用指南：在修改交换机对 supplicant 的重认证时间间隔时，必须首先打开 dot1x

re-authentication。如果没有配置交换机的重认证功能,那么所设置交换机对 supplicant 重认证的时间间隔将不起作用。

举例：设置重认证时间为 1200 秒。

Switch(config)#dot1x timeout re-authperiod 1200

3.28 dot1x timeout tx-period

命令：dot1x timeout tx-period <seconds>

no dot1x timeout tx-period

功能：设置交换机对 supplicant 重发 EAP-request/identity 帧的时间间隔；本命令的 no 操作作为恢复缺省值。

参数：<seconds>为重新发送 EAP 请求帧的时间间隔，单位为秒，取值范围为 1~65535。

命令模式：全局配置模式。

缺省情况：缺省为 30 秒。

使用指南：建议使用缺省值。

举例：更改重新发送 EAP 请求帧的时间间隔为 1200 秒。

Switch(config)#dot1x timeout tx-period 1200

3.29 dot1x unicast enable

命令：dot1x unicast enable

no dot1x unicast enable

功能：打开交换机全局 802.1x 单播透传功能；本命令的 no 操作关闭 802.1x 单播透传功能。

命令模式：全局配置模式。

缺省情况：交换机在全局下不打开 802.1x 单播透传功能。

使用指南：如果要对端口进行 802.1x 单播透传功能认证时，首先要打开全局下的 802.1x 功能，然后打开全局 802.1x 单播透传功能，最后再配置相应端口下的 802.1x 功能。

举例：启动交换机的 802.1x 单播透传功能，并且打开 1/1 号端口 802.1x 功能。

Switch(config)#dot1x enable

Switch(config)#dot1x unicast enable

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#dot1x enable

3.30 dot1x web authentication enable

本交换机不支持此命令。

3.31 dot1x web authentication ipv6 passthrough

本交换机不支持此命令。

3.32 dot1x web redirect

本交换机不支持此命令。

3.33 dot1x web redirect enable

本交换机不支持此命令。

3.34 free-mac

命令：free-mac <source mac><wildcard bits>

no free-mac <source mac><wildcard bits>

功能：为交换机添加免认证 mac；本命令的 no 操作为删除免认证 mac。

参数：<source mac>为免认证用户的 mac 地址；

<wildcard bits>为免认证用户 mac 地址的掩码位。

命令模式：全局配置模式。

缺省情况：不配置。

使用指南：对于特殊用户，可以通过配置免认证 mac 来予以放行。作为免认证的用户，不需要进行认证就可以访问所有资源。可以指定一个用户的 mac 地址免认证，通过配置掩码为 ff-ff-ff-ff-ff-ff；也可以配置一些用户的 mac 免认证，通过配置对应掩码位为 0。

举例：配置免认证 MAC 00-01-11-11-11-11。

Switch(config)# free-mac 00-01-11-11-11-11 ff-ff-ff-ff-ff-ff

3.35 show dot1x

命令：show dot1x [interface <interface-list>]

功能：显示有关 dot1x 参数信息，如果后面增加参数信息，则显示相应端口的 dot1x 的状态。

参数：<interface-list>为端口列表。如果无参数，则显示所有端口信息

命令模式：特权和配置模式

使用指南：通过 show dot1x 命令可以查看端口的 dot1x 的相关参数以及端口的 dot1x 的信息。

举例：

1.显示交换机的 dot1x 全局参数信息。

Switch#show dot1x

Global 802.1x Parameters

reauth-enabled	no
reauth-period	3600
quiet-period	10
tx-period	30
max-req	2
authenticator mode	active

Mac Filter Disable

MacAccessList :

dot1x-EAPoR Enable

dot1x-privateclient Disable

dot1x-unicast Disable

dot1x-web authentication Enable

802.1x is enabled on ethernet Ethernet1/1

802.1X is enabled on vlan 1-4094

Authentication Method:Mac based

Max User Number:50000

Status	Authorized
Port-control	Auto
Supplicant	00-03-0F-FE-2E-D3

Authenticator State Machine

State	Authenticated
-------	---------------

Backend State Machine

State	Idle
-------	------

Reauthentication State Machine

State	Stop
-------	------

802.1X is enabled on ethernet Ethernet1/16

Authentication Method:web based

Status	Authorized
Port-control	Auto
Supplicant IP	192.168.1.11

VLAN id 2

显示内容	解释
Global 802.1x Parameters	全局 802.1x 参数信息
reauth-enabled	交换机是否打开重认证功能
reauth-period	重认证时间间隔
quiet-period	静默时间间隔
tx-period	EAP 数据包重传时间间隔
max-req	EAP 数据包重传次数
authenticator mode	交换机认证模式
Mac Filter	交换机是否使能 dot1x 地址过滤功能
MacAccessList :	Dot1x 地址过滤表
dot1x-EAPoR	交换机采用的认证方式（EAP 中继、EAP 本地终结）
dot1x-privateclient	交换机是否支持私有客户端方式
dot1x-web authentication	交换机是否支持 web 认证功能

802.1x is enabled on ethernet Ethernet1/1	显示端口的 dot1x 是否打开
Authentication Method:	端口认证方式（基于 MAC，基于端口，基于 Web）
Status	端口认证状态
Port-control	端口授权状态
Supplicant	认证者 MAC 地址，webbased 方式下为认证者 IP 地址
Authenticator State Machine	Authenticator 状态机状态
Backend State Machine	Backend 状态机状态
Reauthentication State Machine	Reauthentication 状态机状态

3.36 show dot1x user

命令：show dot1x user

功能：显示已经通过 dot1x 认证的在线用户信息。

命令模式：全局和特权配置模式。

使用指南：一般只关心在线用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。

举例：显示已经通过 dot1x 认证的在线用户信息

Switch(config)# show dot1x user

```

----- total authenticated users: 0 -----
  UserName      Port      OnTime(sec)    MAC      UserIP      UserIPv6
-----
----- total authenticated users: 0-----

```

3.37 clear dot1x

命令：clear dot1x {all |interface <ethernet IFNAME | IFNAME>|mac WORD |user WORD }

功能：删除已经通过 dot1x 认证的在线用户。

参数：<all>：删除所有的 dot1x 在线用户

<IFNAME>：删除指定端口上的 dot1x 在线用户

mac <WORD>：删除指定的 mac 地址的 dot1x 在线用户

user <WORD>：删除指定的用户名的 dot1x 在线用户

命令模式：特权模式。

使用指南：用户使用该命令可以从交换机上删除指定的mac地址、指定的端口、指定的用户名或者所有的dot1x在线用户。

举例：删除所有在线的 dot1x 用户

Switch#clear dot1x all

3.38 user-control limit

本交换机不支持此命令。

3.39 user-control limit ipv6

本交换机不支持此命令。

3.40 vlan-pool

命令： vlan-pool <1-255> WORD

no vlan-pool <1-255>

功能： 新建 vlan 池，本命令的 no 操作为删除建立的 vlan 池。

参数： <1-255> : vlan-pool ID 号（索引）；

WORD: vlan id 列表。

命令模式： 全局配置模式

缺省情况： 交换机不配置 vlan-pool。

使用指南： 在端口下指定 Vlan 开启认证时，首先配置 Vlan 池，在 Vlan 池里指定一个 Vlan 范围，或者某些 Vlan ID，将这个 Vlan 池绑定到端口上，可以指定某个 Vlan 开启认证。新建的 Vlan 池中的元素不能与其他 Vlan 池有重复。不允许更改已经绑定到端口的 Vlan 池里的元素。

举例： 新建 vlan 池 6，包含 vlan id 2-6

Switch (config)#vlan-pool 6 2-6

第 4 章 端口、VLAN 中 MAC、IP 数量限制命令

4.1 debug ip arp count

命令: **debug ip arp count**

no debug ip arp count

功能: 当打开 VLAN 中 arp 数量限制功能 debug 后, VLAN 中动态 arp 的数量、arp 数量已经超出最大允许值的时候都会看到 debug 信息。本命令的 no 操作为 VLAN 中 arp 数量限制功能 debug。

参数: 无。

命令模式: 特权模式。

缺省情况: 缺省没有配置。

使用指南: 通过该命令显示 VLAN 中动态 arp 的数量 debug 信息。

举例:

```
Switch#debug ip arp count
```

```
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!
```

```
%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!
```

4.2 debug ipv6 nd count

命令: **debug ipv6 nd count**

no debug ipv6 nd count

功能: 当打开 VLAN 中 neighbor 数量限制功能 debug 后, VLAN 中动态 neighbor 的数量、neighbor 数量已经超出最大允许值的时候都会看到 debug 信息。本命令的 no 操作为 VLAN 中 neighbor 数量限制功能 debug。

参数: 无。

命令模式: 特权模式。

缺省情况: 缺省没有配置。

使用指南: 通过该命令显示 VLAN 中动态 neighbor 的数量 debug 信息。

举例:

```
Switch#debug ipv6 nd count
```

```
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in vlan 1!!
```

4.3 debug switchport arp count

命令: **debug switchport arp count**

no debug switchport arp count

功能：当打开端口 arp 数量限制功能 debug 后，端口动态 arp 的数量、arp 数量已经超出最大允许值的时候都会看到 debug 信息。本命令的 no 操作为关闭端口 arp 数量限制功能 debug。**参数：**无。

命令模式：特权模式

缺省情况：缺省没有配置。

使用指南：通过该命令显示端口动态 arp 的数量 debug 信息。

举例：

```
Switch#debug switchport arp count
```

```
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit  
in port Ethernet3/1
```

```
!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!
```

4.4 debug switchport mac count

本交换机不支持此命令。

4.5 debug switchport nd count

命令：debug switchport nd count

no debug switchport nd count

功能：当打开端口 nd 数量限制功能 debug 后，端口动态 nd 的数量、nd 数量已经超出最大允许值的时候都会看到 debug 信息。本命令的 no 操作为关闭端口 nd 数量限制功能 debug。

参数：无。

命令模式：特权模式

缺省情况：缺省没有配置。

使用指南：通过该命令显示端口动态 nd 的数量 debug 信息。

举例：

```
Switch#debug switchport arp count
```

```
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum  
limit in port Ethernet3/1
```

```
!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!
```

4.6 debug vlan mac count

本交换机不支持此命令。

4.7 ip arp dynamic maximum

命令：ip arp dynamic maximum <value>

no ip arp dynamic maximum

功能：设置 VLAN 中允许的最大动态 ARP 数量，同时开启 VLAN 中动态 ARP 数量限制功能；本命令的 no 操作为关闭 VLAN 中动态 ARP 数量限制功能。

参数：<value>VLAN 中动态 ARP 数上限，取值范围 1~4096。

缺省情况：关闭 VLAN 中动态 ARP 数量限制功能。

命令模式：接口配置模式

使用指南：配置 VLAN 中允许的最大动态 ARP 数量时，如果 VLAN 中学习的动态 ARP 数量已经大于将要配置的最大数量，将删除多出来的动态 ARP。

举例：

VLAN 1 中打开动态 ARP 数量限制功能，配置最大数量 50 个。

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

```
Switch(Config-if-Vlan1)# ip arp dynamic maximum 50
```

VLAN 1 中关闭动态 ARP 数量限制功能。

```
Switch(Config-if-Vlan1)#no ip arp dynamic maximum
```

4.8 ipv6 nd dynamic maximum

命令：ipv6 nd dynamic maximum <value>

no ipv6 nd dynamic maximum

功能：设置 VLAN 中允许的最大动态 NEIGHBOR 数量，同时开启 VLAN 中动态 NEIGHBOR 数量限制功能；本命令的 no 操作为关闭 VLAN 中动态 NEIGHBOR 数量限制功能。

参数：<value>VLAN 中动态 NEIGHBOR 数上限，取值范围 1~4096。

缺省情况：关闭 VLAN 中动态 NEIGHBOR 数量限制功能。

命令模式：接口配置模式

使用指南：配置 VLAN 中允许的最大动态 NEIGHBOR 数量时，如果 VLAN 中学习的动态 NEIGHBOR 数量已经大于将要配置的最大数量，将删除多出来的动态 NEIGHBOR。

举例：

VLAN 1 中打开动态 NEIGHBOR 数量限制功能，配置最大数量 50 个。

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

```
Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50
```

VLAN 1 中关闭动态 NEIGHBOR 数量限制功能。

```
Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum
```

4.9 mac-address query timeout

本交换机不支持此命令。

4.10 show arp-dynamic count

命令：show arp-dynamic count { (vlan <1-4096>)| interface ethernet <portName>}

功能：显示相应端口、VLAN 中的动态 ARP 数量。

参数：<vlan-id>为显示指定 vlan 标识，<portName>为二层端口名称。

命令模式：特权和配置模式。

使用指南：通过该命令显示出端口、VLAN 中动态 ARP 的数量。

举例：显示配置了 ARP 数量限制功能的端口和 VLAN 中的动态 ARP 数量。

```
Switch(config)#show arp-dynamic count interface ethernet 1/3
```

Port	MaxCount	CurrentCount
Ethernet1/3	5	1

Switch(config)# show arp-dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

4.11 show mac-address dynamic count

本交换机不支持此命令。

4.12 show nd-dynamic count

命令：show nd-dynamic count { (vlan <1-4096>)| interface ethernet <portName>}

功能：显示相应端口、VLAN 中的动态 ND 数量。

参数：<vlan-id>为显示指定 vlan 标识，<portName>为二层端口名称。

命令模式：特权和配置模式。

使用指南：通过该命令显示出端口、VLAN 中动态 ND 的数量。

举例：显示配置了 ND 数量限制功能的端口和 VLAN 中的动态 ND 数量。

Switch(config)#show nd-dynamic count interface ethernet 1/3

Port	MaxCount	CurrentCount
Ethernet1/3	5	1

Switch(config)# show nd-dynamic count vlan 1

Vlan	MaxCount	CurrentCount
1	55	15

4.13 switchport arp dynamic maximum

命令：switchport arp dynamic maximum <value>

no switchport arp dynamic maximum

功能：设置端口允许的最大动态 ARP 数量，同时开启端口动态 ARP 数量限制功能；本命令的 no 操作为关闭端口动态 ARP 数量限制功能。

参数：<value> 端口动态 ARP 数量上限，取值范围 1~4096。

缺省情况：关闭端口动态 ARP 数量限制功能。

命令模式：端口配置模式

使用指南：配置端口允许的最大动态量数量时，如果端口学习的动态量数量已经大于将要配

置的最大数量，将删除多出来的动态 ARP。汇聚端口不支持该功能。

举例：

端口 Ethernet 1/2 模式上打开动态 ARP 数量限制功能，配置最大数量 20 个。

```
Switch(config)#interface ethernet 1/2
```

```
Switch(Config-If-Ethernet1/2)#switchport arp dynamic maximum 20
```

端口 1/2 模式上关闭动态 ARP 数量限制功能。

```
Switch(Config-If-Ethernet1/2)#no switchport arp dynamic maximum
```

4.14 switchport mac-address dynamic maximum

本交换机不支持此命令。

4.15 switchport mac-address violation

本交换机不支持此命令。

4.16 switchport nd dynamic maximum

命令： switchport nd dynamic maximum <value>

no switchport nd dynamic maximum

功能： 设置端口允许的最大动态 NEIGHBOR 数量，同时开启端口动态 NEIGHBOR 数量限制功能；本命令的 no 操作为关闭端口动态 NEIGHBOR 数量限制功能。

参数： <value> 端口动态 NEIGHBOR 数量上限，取值范围 1~4096。

缺省情况： 关闭端口动态 NEIGHBOR 数量限制功能。

命令模式： 端口配置模式

使用指南： 配置端口允许的最大动态 NEIGHBOR 数量时，如果端口学习的动态量数量已经大于将要配置的最大数量，将删除多出来的动态 NEIGHBOR。汇聚端口不支持该功能。

举例：

端口 1/2 模式上打开动态 NEIGHBOR 数量限制功能，配置最大数量 20 个。

```
Switch(config)#interface ethernet 1/2
```

```
Switch(Config-If-Ethernet1/2)#switchport nd dynamic maximum 20
```

端口 1/2 模式上关闭动态 NEIGHBOR 数量限制功能。

```
Switch(Config-If-Ethernet1/2)#no switchport nd dynamic maximum
```

4.17 vlan mac-address dynamic maximum

本交换机不支持此命令。

第 5 章 AM 配置命令

5.1 am enable

命令: **am enable**

no am enable

功能: 全局启动/关闭 AM 功能。

参数: 无。

缺省情况: 默认不启动 AM 功能。

命令模式: 全局配置模式。

使用指南: 无。

举例: 在交换机上启动 AM 功能。

Switch(config)#am enable

在交换机上关闭 AM 功能。

Switch(config)#no am enable

5.2 am port

命令: **am port**

no am port

功能: 打开/关闭端口上的 AM 功能。

参数: 无。

缺省情况: 所有端口 AM 功能关闭。

命令模式: 端口配置模式。

举例: 在交换机的端口 interface Ethernet 1/3 上打开 AM 功能。

Switch(Config-If-Ethernet 1/3)#am port

在交换机的端口 interface 1/3 上关闭 AM 功能。

Switch(Config-If-Ethernet 1/3)#no am port

5.3 am ip-pool

命令: **am ip-pool <ip-address> <num>**

no am ip-pool <ip-address> <num>

功能: 设置端口的访问管理 IP 地址段, 允许/禁止以该 IP 地址段内的 IP 地址为源 IP 地址的 IP 报文与 ARP 报文通过该端口进行转发。

参数: **<ip-address>** 是 IP 地址池中某段地址范围的起始地址。**<num>** 是从 ip-address 开始的连续的地址数量, 其值不大于 32。

缺省情况: IP 地址池为空。

命令模式: 端口配置模式。

使用指南: 无。

举例: 在交换机的端口 interface Ethernet 1/3 上配置允许对源 ip 地址在起始地址为

10.10.10.1 的连续 10 个 ip 地址范围内的数据包进行转发。

```
Switch(Config-If-Ethernet 1/3)#am ip-pool 10.10.10.1 10
```

5.4 am mac-ip-pool

命令： am mac-ip-pool <mac-address> <ip-address>

no am mac-ip-pool <mac-address> <ip-address>

功能： 设置端口的访问管理 MAC-IP 地址，允许/禁止以该 MAC-IP 地址为源地址的 IP 报文与 ARP 报文通过该端口进行转发。

参数： <mac-address>为源 MAC 地址，<ip-address>为包发送的源 IP 地址，32 位二进制数，用四个隔开的十进制数表示。

缺省情况： MAC-IP 地址池为空。

命令模式： 端口配置模式。

使用指南： 无。

举例： 在交换机的端口 interface Ethernet 1/3 上配置允许对源 mac 地址为 11-22-22-11-11-11，且源 ip 地址为 10.10.10.1 的数据包进行转发。

```
Switch(Config-If-Ethernet 1/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1
```

5.5 no am all

命令： no am all [ip-pool|mac-ip-pool]

功能： 删除全部用户配置的 MAC-IP 地址池或 IP 地址池或两个地址池都删除。

参数： ip-pool 为 IP 地址池，mac-ip-pool 为 MAC-IP 地址池，无参数表示对两个地址池都适用。

缺省情况： 初始情况两个地址池都为空。

命令模式： 全局配置模式。

使用指南： 无。

举例： 删除全部已经配置的 IP 地址池。

```
Switch(config)#no am all ip-pool
```

5.6 show am

命令： show am [interface <interface-name>]

功能： 显示已经配置的 AM 入口表项。

参数： <interface-name>为要显示 AM 配置信息的物理接口名，无参数表示显示所有接口的 AM 配置信息。

命令模式： 特权和配置模式。

举例： 显示当前所有已经配置的 AM 入口表项。

```
Switch#show am
```

```
AM is enabled
```

```
Interface Ethernet1/3
```

```
        am port
        am ip-pool 30.10.10.1 20
Interface Ethernet1/5
        am port
        am ip-pool 50.10.10.1 30
        am mac-ip-pool 00-02-04-06-08-09 20.10.10.5
        am ip-pool 50.20.10.1 20
Interface Ethernet1/6
        am port
Interface Ethernet1/1
        am port
        am ip-pool 10.10.10.1 20
        am ip-pool 10.20.10.1 20
```

显示交换机端口 ethernet1/5 的 AM 配置入口表项。

```
Switch#show am interface ethernet 1/5
```

AM is enabled

```
Interface Ethernet1/5
        am port
        am ip-pool 50.10.10.1 30
        am mac-ip-pool 00-02-04-06-08-09 20.10.10.5
        am ip-pool 50.20.10.1 20
```

第 6 章 安全特性配置命令

6.1 dosattack-check srcip-equal-dstip enable

命令： **[no] dosattack-check srcip-equal-dstip enable**

功能： 使能交换机检查源 IP 地址等于目的 IP 地址功能；本命令的 no 操作为关闭检查源 IP 地址等于目的 IP 地址功能。

参数： 无。

缺省情况： 交换机不打开检查源 IP 地址等于目的 IP 地址功能。

命令模式： 全局配置模式。

使用指南： 开启该功能可以丢弃源 IP 地址等于目的 IP 地址的数据报。

举例： 丢弃源 IP 地址等于目的 IP 地址的数据报。

Switch(config)# dosattack-check srcip-equal-dstip enable

6.2 dosattack-check ipv4-first-fragment enable

命令： **[no] dosattack-check ipv4-first-fragment enable**

功能： 使能交换机的检查 IPv4 第一个分片包文的功能；本命令的 no 操作为关闭检查 IPv4 第一个分片包文的功能。

参数： 无。

缺省情况： 交换机不打开检查 IPv4 第一个分片包文的功能。

命令模式： 全局配置模式。

使用指南： 该功能单独使用没有任何作用，需要与命令 **dosattack-check tcp-flags enable** 或命令 **dosattack-check srcport-equal-dstport enable** 结合使用。

举例： 丢弃 IPv4 分片和不分片的源端口等于目的端口的数据报。

Switch(config)# dosattack-check ipv4-first-fragment enable

Switch(config)# dosattack-check srcport-equal-dstport enable

6.3 dosattack-check tcp-flags enable

命令： **[no] dosattack-check tcp-flags enable**

功能： 使能交换机的检查非法 TCP 标志功能；本命令的 no 操作为关闭检查非法 TCP 标志功能。

参数： 无。

缺省情况： 交换机不打开检查非法 TCP 标志功能。

命令模式： 全局配置模式。

使用指南： 开启该功能后交换机可以丢弃下述 4 种包含非法 TCP 标志的数据报：SYN=1 且源端口小于 1024；TCP 标志位全为 0 且序列号等于 0；FIN=1，URG=1，PSH=1 且 TCP 序列号=0；SYN=1 且 FIN=1。该功能可以与 dosattack-check ipv4-first-fragment enable 结合使用，可以阻止 ipv4 分片的包含非法 TCP 标志的数据报。

举例： 丢弃上述 4 种类型报文中的 1 种或若干种。

Switch(config)# dosattack-check tcp-flags enable

6.4 dosattack-check srcport-equal-dstport enable

命令： dosattack-check srcport-equal-dstport enable

no dosattack-check srcport-equal-dstport enable

功能： 使能交换机的检查源端口等于目的端口功能；本命令的 no 操作为关闭检查源端口等于目的端口功能。

参数： 无。

缺省情况： 交换机不打开检查源端口等于目的端口功能。

命令模式： 全局配置模式。

使用指南： 开启该功能后，交换机可以丢弃目的端口等于源端口的 TCP 和 UDP 数据报。该功能可以与 dosattack-check ipv4-first-fragment enable 功能结合使用，可以阻止 IPv4 分片的源端口等于目的端口的 TCP 和 UDP 数据报。

举例： 丢弃不分片的源端口等于目的端口的 TCP/UDP 数据报。

Switch(config)# dosattack-check srcport-equal-dstport enable

6.5 dosattack-check tcp-fragment enable

命令： [no] dosattack-check tcp-fragment enable

功能： 使能交换机的检查 TCP 碎片攻击功能；本命令的 no 操作为关闭检查 TCP 碎片攻击功能。

参数： 无。

缺省情况： 交换机不打开检查 TCP 碎片攻击功能。

命令模式： 全局配置模式。

使用指南： 开启该功能后，交换机可以防止 TCP 碎片攻击，丢弃 TCP 分片的偏移值为 1 的数据报文和 TCP 报文段长度(TCP 头部和载荷)小于指定长度并且是第一个分片的 TCP 数据报文。指定长度由命令 dosattack-check tcp-segment 设置。

举例： 打开检查 TCP 碎片攻击功能。

Switch(config)# dosattack-check tcp-fragment enable

6.6 dosattack-check tcp-segment

命令： dosattack-check tcp-segment <20-255>

功能： 设置交换机允许通过的最小 TCP 报文段长度。

参数： <20-255> 为交换机允许通过的最小 TCP 报文段长度。

缺省情况： 缺省值为 20，最小的 TCP 报文段长度。

命令模式： 全局配置模式。

使用指南： 使用该功能的前提必须开启 dosattack-check tcp-fragment enable 功能。

举例： 设置允许通过的最小 TCP 报文段长度是 20。

Switch(config)# dosattack-check tcp-fragment enable

Switch(config)# dosattack-check tcp-segment 20

6.7 dosattack-check icmp-attacking enable

命令： `[no] dosattack-check icmp-attacking enable`

功能： 使能交换机的检查 ICMP 碎片攻击功能；本命令的 `no` 操作为关闭检查 ICMP 碎片攻击功能。

参数： 无。

缺省情况： 交换机不打开检查 ICMP 碎片攻击功能。

命令模式： 全局配置模式。

使用指南： 开启该功能后，交换机可以防止 ICMP 碎片攻击，丢弃分片的 ICMP 报文和 ICMP 净荷长度大于指定长度的 ICMPv4/v6 的数据报。

举例： 开启检查 ICMP 碎片攻击功能。

Switch(config)# dosattack-check icmp-attacking enable

6.8 dosattack-check icmpV4-size

命令： `dosattack-check icmpV4-size <64-1023>`

功能： 设置交换机允许通过的最大 ICMPv4 数据报净荷长度。

参数： `<64-1023>` 为交换机允许通过的最大 ICMPv4 数据报净荷长度。

缺省情况： 缺省值为 0x200。

命令模式： 全局配置模式。

使用指南： 使用该功能的前提是必须开启 `dosattack-check icmp-attacking enable`。

举例： 设置交换机允许通过的最大 ICMPv4 数据报净荷长度为 100。

Switch(config)# dosattack-check icmp-attacking enable

Switch(config)# dosattack-check icmpV4-size 100

6.9 dosattack-check icmpv6-size

命令： `dosattack-check icmpv6-size <64-1023>`

功能： 设置交换机允许通过的最大 ICMPv6 数据报净荷长度。

参数： `<64-1023>` 为交换机允许通过的最大 ICMPv6 数据报净荷长度。

缺省情况： 缺省值为 0x200。

命令模式： 全局配置模式。

使用指南： 使用该功能的前提是必须开启 `dosattack-check icmp-attacking enable`。

举例： 设置交换机允许通过的最大 ICMPv6 数据报净荷长度为 100。

Switch(config)#dosattack-check icmp-attacking enable

Switch(config)#dosattack-check icmpv6-size 100

第 7 章 TACACS+命令

7.1 tacacs-server authentication host

命令： `tacacs-server authentication host <ip-address> [port <port-number>] [timeout <seconds>] [key {0 | 7} <string>] [primary]`

no tacacs-server authentication host <ip-address>

功能： 设置 TACACS+服务器 IP 地址、监听端口号、认证服务器超时时间、密钥字符串；本命令的 no 操作为删除 TACACS+认证服务器。

参数： **<ip-address>** 服务器的 IP 地址；**<port-number>** 为服务器的监听端口号，取值范围为 0~65535，其中 0 表示不作认证服务器使用；**<seconds>** 为 TACACS+认证超时定时器值，单位为秒，取值范围为 1~60；**<string>** 为密钥字符串，如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符，如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符；**primary** 为主用服务器。

命令模式： 全局配置模式。

缺省情况： 系统没有设置 TACACS+认证服务器。

使用指南： 本命令用于指定与交换机进行认证的 TACACS+服务器的 IP 地址、端口号、认证服务器超时时间和密钥字符串，可以配置多条该命令。其中参数 **port** 用于指定认证端口号，该端口号必须与指定的 TACACS+服务器上的认证端口号相同，缺省为 49，参数 **key** 和 **timeout**，用于设置该服务器自身单独的 **key** 和 **timeout**，如果不配置这两个参数，缺省使用 **tacacs-server key <string>**，**tacacs-server timeout <seconds>** 全局配置命令；本命令可以反复配置多条以指定多台与交换机建立通讯关系的 TACACS+服务器，其中以配置的顺序作为交换机认证服务器的顺序。如果配置 **primary**，则将此 TACACS+服务器作为主用服务器。

举例： 配置 TACACS+认证服务器地址为 192.168.1.2，且使用全局配置的 **key**。

Switch(config)#tacacs-server authentication host 192.168.1.2

7.2 tacacs-server key

命令： `tacacs-server key {0 | 7} <string>`

no tacacs-server key

功能： 设置 TACACS+认证服务器的密钥；本命令的 no 操作为删除 TACACS+服务器的密钥。

参数： **<string>** 为 TACACS+服务器的密钥字符串，如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符，如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

命令模式： 全局配置模式。

使用指南： 该密钥为交换机与 TACACS+服务器进行加密的报文通信使用。该设置的密钥必须与 TACACS+服务器上的密钥相同，否则将不能进行正确的 TACACS+认证。为保证 TACACS+认证数据的安全，建议配置认证服务器密钥。

举例：配置 TACACS+服务器认证密钥为 test。

```
Switch(config)# tacacs-server key 0 test
```

7.3 tacacs-server nas-ipv4

命令：tacacs-server nas-ipv4 <ip-address>

no tacacs-server nas-ipv4

功能：设置交换设备发送 TACACS+报文的 IP 源地址。本命令的 no 操作用来删除该配置。

参数：<ip-address>为指定发送 TACACS+报文使用的 IP 源地址，点分十进制格式，必须为合法的单播地址。

缺省情况：没有配置特定的 IP 源地址，TACACS+报文源地址使用发送接口的 IP 地址。

命令模式：全局配置模式。

使用指南：配置的源地址必须为本机的 IP 地址，否则发送 TACACS+报文时会返回无法绑定 IP 地址的错误提示。推荐使用 loopback 接口的地址作为源地址，这样可以避免物理接口 down 时 TACACS+服务器返回的报文不可达。

举例：配置交换设备发送 TACACS+报文使用源地址 192.168.2.254。

```
Switch#tacacs-server nas-ipv4 192.168.2.254
```

7.4 tacacs-server timeout

命令：tacacs-server timeout <seconds>

no tacacs-server timeout

功能：设置 TACACS+服务器认证超时定时器；本命令的 no 操作为恢复缺省配置。

参数：<seconds>为 TACACS+认证超时定时器值，单位为秒，取值范围为 1~60。

命令模式：全局配置模式。

缺省情况：缺省为 3 秒。

使用指南：本命令指定交换机通过 TACACS+服务器认证的等待时间。交换机建立到 TACACS+的连接，向 TACACS+ Server 发送请求认证数据包后，等待接收相应的响应数据包。若在规定的等待时间内没有建立连接或者没有接收到 TACACS+服务器的回应，则认为这次认证失败。

举例：配置 tacacs+服务器超时定时器为 30 秒。

```
Switch(config)#tacacs-server timeout 30
```

7.5 debug tacacs-server

命令：debug tacacs-server

no debug tacacs-server

功能：打开 TACACS+的调试信息；本命令的 no 操作为关闭 TACACS+的调试信息。

命令模式：特权配置模式。

参数：无。

使用指南：打开 TACACS+调试信息，可以查看 TACACS+协议的协商过程，在遇到故障时有助于监测故障原因。

举例：打开 TACACS+协议的调试信息。

```
Switch#debug tacacs-server
```

第 8 章 RADIUS 配置命令

8.1 aaa enable

命令：aaa enable

no aaa enable

功能：使能交换机 AAA 认证功能；本命令的 no 操作为关闭 AAA 认证功能。

命令模式：全局配置模式。

参数：无。

缺省情况：交换机不打开 AAA 认证功能。

使用指南：如果要想实现交换机的 802.1x 认证功能，必须打开交换机的 AAA 认证功能。

举例：打开交换机的 AAA 功能。

Switch(config)#aaa enable

8.2 aaa-accounting enable

命令：aaa-accounting enable

no aaa-accounting enable

功能：打开交换机的 AAA 计费功能；本命令的 no 操作为关闭 AAA 计费功能。

命令模式：全局配置模式。

缺省情况：交换机不打开 AAA 计费功能。

使用指南：打开交换机的计费功能后，交换机将对认证者所在的端口的流量信息或上网时间进行计费。在计费开始时，交换机向 Radius 计费服务器发出计费开始的消息；并且每隔 5 秒钟针对在线用户向 Radius 计费服务器发一次计费包；在计费停止时，又向 Radius 计费服务器发送计费停止的消息。注意：只有当计费功能打开时，交换机在用户下线时才通知 Radius 计费服务器，用户的下线消息并不会通知 Radius 认证服务器。

举例：打开交换机的 AAA 计费功能。

Switch(config)#aaa-accounting enable

8.3 aaa-accounting update

命令：aaa-accounting update {enable|disable}

功能：打开或关闭交换机的 AAA 计费更新功能。

命令模式：全局配置模式。

缺省情况：交换机打开 AAA 计费更新功能。

使用指南：打开交换机的计费更新功能后，对于每个在线用户，交换机将定时向计费服务器发送计费报文。

举例：关闭交换机的 AAA 计费更新功能。

Switch(config)#aaa-accounting update disable

8.4 aaa group server radius

命令：aaa group server radius <WORD>

no aaa group server radius <WORD>

功能：使用该命令配置一个 aaa radius 服务器组名称，并进入 aaa radius 服务器组配置模式，该命令的 no 形式删除这个 aaa radius 服务器组。

参数：WORD: aaa group server radius 的名字，它是一个长度不大于 32 的字符串, (a-z, A-Z, 0-9, '_', '-', and space are allowed)

缺省情况：无。

命令模式：全局配置模式

使用指南：使用该命令配置一个 aaa radius 服务器组。

举例：使用该命令配置一个 aaa radius 服务器组，组名为 group1。

Switch (Config)# aaa group server radius group1

8.5 debug aaa packet

命令：debug aaa packet {send|receive|all} interface {ethernet <interface-number>|<interface-name>}

no debug aaa packet {send|receive|all} interface {ethernet <interface-number>|<interface-name>}

功能：打开 aaa 的收发包调试信息；本命令的 no 操作为关闭 aaa 的收发包调试信息。

参数：send: 打开 aaa 的发包调试信息。
receive: 打开 aaa 的收包调试信息。
all: 打开 aaa 的收包和发包调试信息。
<interface-number>: 端口序号。
<interface-name>: 端口名称。

命令模式：特权配置模式。

使用指南：打开 aaa 收发包调试信息，可以查看 Radius 协议收到的和发出的报文，在遇到故障时有助于监测故障原因。

举例：打开端口 1/1 下 aaa 所有收发包调试信息。

Switch#debug aaa packet all interface Ethernet 1/1

8.6 debug aaa detail attribute

命令：debug aaa detail attribute interface {ethernet <interface-number>|<interface-name>}

no debug aaa detail attribute interface {ethernet <interface-number>|<interface-name>}

功能：打开 aaa 的 Radius 属性细节调试信息；本命令的 no 操作为关闭 aaa 的 Radius 属性细节调试信息。

参数：<interface-number>: 端口序号。
<interface-name>: 端口名称。

命令模式：特权配置模式。

使用指南：打开 aaa 的 Radius 属性细节调试信息，可以查看 Radius 报文的 Radius 属性细节，在遇到故障时有助于监测故障原因。

举例：打开端口 1/1 下 aaa 的 Radius 属性细节调试信息。

Switch#debug aaa detail attribute interface Ethernet 1/1

8.7 debug aaa detail connection

命令：debug aaa detail connection

no debug aaa detail connection

功能：打开 aaa 的连接细节调试信息；本命令的 no 操作为关闭 aaa 的连接细节调试信息。

参数：无。

命令模式：特权配置模式。

使用指南：打开 aaa 连接细节调试信息，可以查看 aaa 的连接细节信息，在遇到故障时有助于监测故障原因。

举例：打开 aaa 连接细节调试信息。

Switch#debug aaa detail connection

8.8 debug aaa detail escape

命令：debug aaa detail escape

功能：打开 radius server 逃生功能调试信息。本命令的 no 操作为关闭 radius server 逃生功能调试信息。

命令模式：特权配置模式。

使用指南：打开逃生功能调试信息，可以查看 aaa 模块对 radius server 的周期性探测，在遇到故障时有助于监测故障原因。

举例：打开 radius server 逃生功能调试信息。

Switch#debug aaa detail escape

8.9 debug aaa detail event

命令：debug aaa detail event

no debug detail event

功能：打开 aaa 的事件调试信息；本命令的 no 操作为关闭 aaa 的事件调试信息。

参数：无。

命令模式：特权配置模式。

使用指南：打开 aaa 事件调试信息，可以查看 Radius 协议运行过程产生的各种事件信息，在遇到故障时有助于监测故障原因。

举例：打开 aaa 的事件调试信息。

Switch#debug aaa detail event

8.10 debug aaa error

命令：debug aaa error

no debug error

功能：打开 aaa 的出错调试信息；本命令的 no 操作为关闭 aaa 的出错调试信息。

参数：无。

命令模式：特权配置模式。

使用指南：打开 aaa 出错调试信息，可以查看 Radius 协议运行过程中产生的各种出错信息，在遇到故障时有助于监测故障原因。

举例：打开 aaa 出错调试信息。

Switch#debug aaa error

8.11 radius nas-ipv4

命令：radius nas-ipv4 <ip-address>

no radius nas-ipv4

功能：设置交换设备发送 RADIUS 报文的 IP 源地址。本命令的 no 操作用来删除该配置。

参数：<ip-address>为指定发送 RADIUS 报文使用的 IP 源地址，点分十进制格式，必须为合法的单播地址。

缺省情况：没有配置特定的 IP 源地址，RADIUS 报文源地址使用发送接口的 IP 地址。

命令模式：全局配置模式。

使用指南：配置的源地址必须为本机的 IP 地址，否则发送 RADIUS 报文时会返回无法绑定 IP 地址的错误提示。推荐使用 loopback 接口的地址作为源地址，这样可以避免物理接口 down 时 RADIUS 服务器返回的报文不可达。

举例：配置交换设备发送 RADIUS 报文使用源地址 192.168.2.254。

Switch#radius nas-ipv4 192.168.2.254

8.12 radius nas-ipv6

命令：radius nas-ipv6 <ipv6-address>

no radius nas-ipv6

功能：设置交换设备发送 RADIUS 报文的 IPv6 源地址。本命令的 no 操作用来删除该配置。

参数：<ipv6-address> 为指定发送 RADIUS 报文使用的 IPv6 源地址，必须为合法的单播地址。

缺省情况：没有配置特定的 IPv6 源地址，RADIUS 报文源地址使用发送接口的 IPv6 地址。

命令模式：全局配置模式

使用指南：配置的源地址必须为本机的 IPv6 地址，否则发送 RADIUS 报文时会返回无法绑定 IPv6 地址的错误提示。推荐使用 loopback 接口的地址作为源地址，这样可以避免物理接口 down 时 RADIUS 服务器返回的报文不可达。

举例：配置交换设备发送 RADIUS 报文使用 IPv6 源地址 2001:da8:456::1。

Switch#radius nas-ipv6 2001:da8:456::1

8.13 radius-server accounting host

命令：radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary]

no radius-server accounting host {<ipv4-address> | <ipv6-address>}

功能：设置 RADIUS 计费服务器 IPv4 或者 IPv6 地址和监听端口号、是否为主用服务器；本命令的 no 操作为删除 RADIUS 计费服务器。

参数：{<ipv4-address> | <ipv6-address>} 服务器的 IPv4 地址或者 IPv6 地址。

<port-number> 为服务器的监听端口号，取值范围为 0~65535。

<string> 为密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

[primary] 是否设为主用服务器，在配置 radius server 时，可以配置多个，使用顺序如果不配置 primary 时，按配置顺序查找可以使用的 radius server。如果配置的 primary，则首先使用这个 radius server。

命令模式：全局配置模式。

缺省情况：系统没有设置 RADIUS 计费服务器。

使用指南：本命令用于指定与交换机进行计费的 RADIUS 服务器的 IPv4 地址或者 IPv6 地址和端口号，可以配置多条该命令。其中参数<port-number>用于指定计费端口号，该端口号必须与指定的 RADIUS 服务器上的计费端口号相同，缺省为 1813，

若将该端口号配置为 0，端口随机产生，可能导致无效。本命令可以反复配置多条以指定多台与交换机建立通讯关系的 RADIUS 服务器，交换机将向所有配置好的计费服务器发送计费报文，所配置的这些 RADIUS 计费服务器可以相互作为备份服务器。如果配置 primary，则将此 RADIUS 服务器作为主用服务器。只能配置一个 RADIUS 主服务器，不管该服务器使用 IPv4 还是 IPv6 地址。

举例：设置 RADIUS 计费服务器的 IPv6 地址为 2004:1:2:3::2，端口号为 3000，并作为主用服务器。

Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary

8.14 radius-server authentication host

命令：radius-server authentication host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}]

no radius-server authentication host {<ipv4-address> | <ipv6-address>}

功能：设置 RADIUS 认证服务器 IPv4 地址或者 IPv6 地址和监听端口号、加密密钥、是否为主用服务器以及使用模式；本命令的 no 操作为删除 RADIUS 服务器。

参数：{<ipv4-address> | <ipv6-address>} 服务器的 IPv4 地址或者 IPv6 地址。

<port-number> 为服务器的监听端口号，取值范围为：0~65535。

<string> 为密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

[primary]是否设为主用服务器，在配置 radius server 时，可以配置多个，使用顺序如果不配置 primary 时，按配置顺序查找可以使用的 radius server。如果配置的 primary，

则首先使用最后配置的这个 radius server。

[access-mode {dot1x | telnet}] 指明当前 RADIUS 服务器只为 802.1x 认证或 telnet 远程认证使用，默认所有服务均可使用当前 RADIUS 服务器。

命令模式：全局配置模式。

缺省情况：系统没有设置 RADIUS 认证服务器。

使用指南：本命令用于指定与交换机进行认证的 RADIUS 服务器的 IPv4 地址或者 IPv6 地址和端口号以及密钥字符串和访问模式，可以配置多条该命令。其中参数 **<port-number>** 用于指定认证端口号，该端口号必须与指定的 RADIUS 服务器上的认证端口号相同，缺省为 1812，若将该端口号配置为 0 端口随机产生，可能导致无效。本命令可以反复配置多条以指定多台与交换机建立通讯关系的 RADIUS 服务器，其中以配置的顺序作为交换机认证服务器的顺序，当第一服务器有响应（无论是认证成功或失败）时，交换机不向下一个服务器发送认证请求。如果配置 **primary**，则将此 RADIUS 服务器作为主用服务器。当前 RADIUS 服务器若没有配置 **key <string>**，则使用命令 **radius-server key <string>** 全局配置的密钥。另外，还可以通过 **access-mode** 选项指定当前 RADIUS 服务器只为 802.1x 认证或 telnet 远程认证使用。默认不配置 **access-mode** 选项，所有远程认证服务均可使用该 RADIUS 服务器。

举例：配置 RADIUS 认证服务器的 IPv6 地址为 2004:1:2:3::2。

Switch(config)#radius-server authentication host 2004:1:2:3::2

8.15 radius-server dead-time

命令：radius-server dead-time <minutes>

no radius-server dead-time

功能：设置 RADIUS 服务器死机后的恢复时间；本命令的 **no** 操作为恢复缺省配置。

参数：<minutes>为 RADIUS 服务器死机的恢复时间值，单位为分钟，取值范围为 1~255。

命令模式：全局配置模式。

缺省情况：缺省为 5 分钟。

使用指南：本命令指定交换机等待 RADIUS 服务器由不可访问状态恢复为可以访问状态的时间。交换机查知该服务器不能访问时，交换机将该服务器状态设置成无效状态，超过上述配置间隔时间后，系统将认证服务器状态设置成有效。

举例：配置 RADIUS 服务器死机后的恢复时间为 3 分钟。

Switch(config)#radius-server dead-time 3

8.16 radius-server key

命令：radius-server key {0 | 7} <string>

no radius-server key

功能：设置 RADIUS 服务器（包括认证和计费）的密钥；本命令的 **no** 操作为删除 RADIUS 服务器的密钥。

参数：<string> 为 RADIUS 服务器的密钥字符串。如果密钥类型选项为 0，则后续指定明文密钥，取值范围不超过 64 个字符；如果选项为 7，则后续指定为明文密钥加密后的密文字串，该密文字串解密后对应的明文长度不超过 64 个字符。

命令模式：全局配置模式。

使用指南： 该密钥为交换机与设置的 RADIUS 服务器进行加密的报文通信使用。该设置的密钥必须与交换机设置的 RADIUS 服务器上的密钥相同，否则将不能进行正确的 RADIUS 认证和计费。

举例： 配置 RADIUS 认证密钥为 test。

Switch(config)#radius-server key 0 test

8.17 radius-server retransmit

命令： radius-server retransmit <retries>

no radius-server retransmit

功能： 设置 RADIUS 认证报文的重传次数；本命令的 no 操作为恢复缺省配置。

参数： <retries>为 RADIUS 服务器的重传次数，取值范围为 0~100。

命令模式： 全局配置模式。

缺省情况： 缺省为 3 次。

使用指南： 本命令指定交换机向 RADIUS 服务器发送数据包后，接收不到 RADIUS 服务器的回应需要重新发送该数据包的次数。在没有收到认证服务器发送的认证信息时，需向认证服务器重传 AAA 的认证请求。重传 AAA 请求计数达到设定的重传次数并仍没有接收到服务器的回应后，认为该服务器已不能正常工作，交换机将该服务器设置为不可访问状态。

举例： 配置 RADIUS 认证报文重传次数为 5 次。

Switch(config)#radius-server retransmit 5

8.18 radius-server timeout

命令： radius-server timeout <seconds>

no radius-server timeout

功能： 设置 RADIUS 服务器超时定时器；本命令的 no 操作为恢复缺省配置。

参数： <seconds>为 RADIUS 服务器超时定时器值，单位为秒，取值范围为 1~1000。

命令模式： 全局配置模式。

缺省情况： 缺省为 3 秒。

使用指南： 本命令指定交换机等待 RADIUS 服务器响应的时间间隔。交换机发送给 RADIUS Server 的请求数据包后，等待接收相应的响应数据包。若在规定的等待时间内没有接收到 RADIUS 服务器的回应，则根据当时的状态重新发送请求数据包或将该服务器状态设置为不可访问。

举例： 配置 RADIUS 服务器超时定时器为 30 秒。

Switch(config)#radius-server timeout 30

8.19 radius-server accounting-interim-update timeout

命令： radius-server accounting-interim-update timeout <seconds>

no radius-server accounting-interim-update timeout

功能： 设置计费更新报文发送的时间间隔；本命令的 no 操作为恢复缺省配置。

参数： <seconds>为计费更新报文发送的时间间隔，单位为秒，取值范围为 60~3600。

命令模式：全局配置模式。

缺省情况：缺省的计费更新报文发送的时间间隔为 300 秒。

使用指南：本命令指定 NAS 发送计费更新报文的时间间隔。为了对用户实施实时计费，从用户上线时间开始，每间隔设定的时间，NAS 会向 RADIUS 服务器发送一次该在线用户的计费更新报文。

计费更新报文发送时间间隔的取值与NAS支持的最大用户数有一定的相关性要求——取值越小，NAS支持的最大用户数也就越少；取值越大，NAS支持的最大用户数也就越多。以下是计费更新报文发送时间间隔与最大用户数之间的推荐比例关系：

表 8-1 计费更新报文发送时间间隔与用户量之间的推荐比例关系

最大用户数	计费更新报文发送时间间隔（秒）
1~299	300（缺省值）
300~599	600
600~1199	1200
1200~1799	1800
≥1800	3600

举例：NAS 支持的最大用户数为 700 人，配置计费更新报文发送的时间间隔为 1200 秒。
Switch(config)#radius-server accounting-interim-update timeout 1200

8.20 server

命令：server <A.B.C.D>
no server <A.B.C.D>

功能：使用该命令添加 aaa radius 服务器组的服务器，no 形式删除该服务器。

参数：<A.B.C.D>: server 的 IP 地址

缺省情况：无

命令模式：aaa radius 服务器组配置模式

使用指南：使用该命令在 aaa radius 服务器组中添加 radius 服务器地址

举例：使用该命令在 aaa radius 服务器组 group1 中添加一个 radius 服务器，IP 地址为 192.168.10.1
Switch (Config)# aaa group server radius group1
Switch (config-sg-radius)# server 192.168.10.1

8.21 show aaa authenticated-user

命令：show aaa authenticated-user

功能：显示已经通过认证的在线用户。

命令模式：特权和配置模式。

使用指南：一般只关心在线用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。

举例：
Switch#show aaa authenticated-user
----- authenticated users -----

```

UserName  Retry RadID Port EapID ChapID OnTime  UserIP      MAC
-----
----- total: 0 -----

```

8.22 show aaa authenticating-user

命令：show aaa authenticating-user

功能：显示正在进行认证的用户。

命令模式：特权和配置模式。

使用指南：一般只关心正在进行认证用户的信息，其它显示信息为技术支持人员用于故障诊断和排错。

举例：

Switch#show aaa authenticating-user

```

----- authenticating users -----
User-name  Retry-time  Radius-ID  Port  Eap-ID Chap-ID Mem-Addr  State
-----
----- total: 0 -----

```

8.23 show aaa config

命令：show aaa config

功能：显示 radius client 已经有的配置命令并包含其中 IPv6 有关信息。

命令模式：特权和配置模式。

使用指南：显示交换机是否打开 aaa 认证、计费功能，及密钥，认证、计费服务器的信息等。

举例：

Switch#show aaa config

显示的内容举例如下（如果是布尔量，1 代表 TRUE，0 代表 FALSE）：

```

----- AAA config data -----

Is Aaa Enabled = 1      : 1 表示 aaa 认证使能，0 表示没被使能
Is Account Enabled= 0   : 1 表示 aaa 计费使能，0 表示没被使能
MD5 Server Key = yanshifeng : 认证密钥
authentication server sum = 2 : 配置的认证服务器的个数
authentication server[0].sock_addr =2:100.100.100.60.1812: 第一个认证服务器的地
址协议族、IP 和端口号

.Is Primary = 1: 是为主用服务器
.Is Server live by radius escape function = 1: 该服务器是
否死掉

.Socket No = 0 : 通向该服务器的本地 socket 号

```

```
authentication server[1].sock_addr = 10:2004:1:2::2.1812
    .Is Primary = 0
    .Is Server live by radius escape function = 1
    .Socket No = 0
accounting server sum = 2 : 配置的计费服务器的个数
accounting server[0].sock_addr = 2:100.100.100.65.1813: 计费服务器的地址协议族、
IP 和端口号
    .Is Primary = 1: 是为主用服务器
    .Socket No = 0: 通向该服务器的本地 socket 号
accounting server[1].sock_addr = 10:2004::7.1813
    .Is Primary = 1
    .Socket No = 0
Retransmit = 4: 超时重传次数
Time Out = 6 (Sec): 发送请求包后, 等待回应超时时间
Dead Time = 5 (min): 对死掉服务器开始重试的时间间隔
Intrim-Update-Accounting Interval = 600(Sec): 计费时间间隔
```

8.24 show radius authenticated-user count

命令: show radius authenticated-user count

功能: 显示已经通过认证的在线用户数量。

命令模式: 特权和配置模式。

举例:

```
Switch#show radius authenticated-user count
```

```
The authenticated online user num is:      105
```

8.25 show radius authenticating-user count

命令: show radius authenticating-user count

功能: 显示正在进行认证的用户数量。

命令模式: 特权和配置模式。

举例:

```
Switch#show radius authenticating-user count
```

```
The authenticating user num is:          10
```

8.26 radius 逃生

8.26.1 radius-server escape { enable | disable }

命令: radius-server escape enable

radius-server escape disable

功能: 使能交换机 AAA 的 radius server 逃生功能。

参数：无。

缺省情况：默认关闭逃生功能。

命令模式：全局配置模式。

使用指南：打开 radius server 逃生功能以后，对于 dot1x 或者 portal 认证客户端来说，当 dot1x 或者 portal 认证客户端上所配置的 radius server 不可达时，此时 dot1x 或者 portal 认证客户端的流量放行。当探测到所配置的认证服务器重新可达时，删除对逃生客户端先前下发的流量放行规则表项。

举例：使能全局认证功能。

Switch (Config)# radius-server escape enable

8.26.2 radius-server escape detection-interval

命令：radius-server escape detection-interval {default| < second >}

功能：配置对 radius server 进行可达性探测的周期。

参数：default:时间间隔恢复成默认的 3 分钟；

second:配置时间间隔值，取值范围为 1-1800 秒。

缺省情况：默认时间是 180 秒。

命令模式：全局配置模式。

使用指南：配置的时间间隔越小，逃生功能越灵敏。但是配置的时间间隔要大于 (Retransmit+1) * Time Out。

举例：配置对 radius server 探测的周期为 120 秒。

Switch(config)#radius-server escape detection-interval 120

第 9 章 SSL 配置命令

9.1 ip http secure-server

命令: **ip http secure-server**

no ip http secure-server

功能: 启动/关闭 SSL 功能。

参数: 无。

命令模式: 全局配置模式。

缺省情况: 缺省为不配置。

使用指南: 本命令用于启动/关闭 SSL 功能。当启动 SSL 功能后, 用户在客户端通过 https 访问交换机时, 交换机就会和客户端进行 SSL 握手连接, 形成安全的 SSL 连接通道, 在此之后应用层协议所传送的数据都会被加密, 从而保证通信的私密性。

举例: 启动 SSL 功能

Switch(config)#ip http secure-server

9.2 ip http secure-port

命令: **ip http secure-port <port-number>**

no ip http secure-port

功能: 配置/删除 SSL 服务监听的端口号。

参数: <port-number>设置的监听端口号, 范围 1025~65535。默认配置为 443。

命令模式: 全局配置模式。

缺省情况: 缺省为不配置。

使用指南: 如果使用了本命令配置了端口号, 则使用配置的端口号进行监听。如果改变了 https 使用的端口号, 用户尝试使用 https 连接的时候必须指定端口号为修改后的, 如: https://device:port_number。端口号的修改每次都需要重启 SSL 功能。

举例: 配置 SSL 使用的端口号 1028。

Switch(config)#ip http secure-port 1028

9.3 ip http secure- ciphersuite

命令: **ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha}**

no ip http secure-ciphersuite

功能: 配置/删除 SSL 使用的加密套件。

参数: **des-cbc3-sha** 加密算法 DES_CBC3, 摘要算法 SHA。

rc4-128-sha 加密算法 RC4_128, 摘要算法 SHA。

des-cbc-sha 加密算法 DES_CBC, 摘要算法 SHA。

默认使用的是 **rc4-md5**。

命令模式: 全局配置模式。

缺省情况: 缺省为不配置。

使用指南：如果使用了本命令配置了加密套件，则使用配置的加密套件进行加密的协商。加密套件的修改每次都需要重启 SSL 功能。使用 des-cbc-sha 加密套件时，必须 ie7.0 以上的浏览器才能支持。

举例：配置 SSL 使用的加密套件 rc4-128-sha。

```
Switch(config)#ip http secure- ciphersuite rc4-128-sha
```

9.4 show ip http secure-server status

命令：show ip http secure-server status

功能：显示配置的 SSL 信息。

参数：无。

命令模式：特权和配置模式。

举例：

```
Switch#show ip http secure-server status
HTTP secure server status: Enabled
HTTP secure server port: 1028
HTTP secure server ciphersuite: rc4-128-sha
```

9.5 debug ssl

命令：debug ssl

no debug ssl

功能：显示使用 SSL 功能信息，该命令的 no 形式关闭 DEBUG 显示。

参数：无。

命令模式：特权模式。

举例：

```
Switch#debug ssl
%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998
%Jan 01 01:02:05 2006 connect to http security server sucess!
```

第 10 章 IPv6 安全 RA 命令

10.1 ipv6 security-ra enable

命令：ipv6 security-ra enable

no ipv6 security-ra enable

功能：全局使能 IPv6 安全 RA 功能，所有的 RA 公告报文不通过硬件转发而是只送 CPU 处理。本命令的 no 操作关闭全局 IPv6 安全 RA 功能。

参数：无。

命令模式：全局配置模式。

缺省情况：默认不启动 IPv6 安全 RA 功能。

使用指南：必须全局启动安全 RA 功能后，在端口上的安全 RA 才能启动。关闭全局安全 RA 后，同时清除掉所有已配置的安全 RA 端口。全局安全 RA 功能与全局 IPv6 SAVI 功能互斥，两者不能同时开启。

举例：全局启动 IPv6 安全 RA。

Switch(config)#ipv6 security-ra enable

10.2 ipv6 security-ra enable

命令：ipv6 security-ra enable

no ipv6 security-ra enable

功能：端口上使能 IPv6 安全 RA 功能，该端口收到的 RA 报文不进行转发处理。本命令的 no 操作关闭端口的 IPv6 安全 RA 功能。

参数：无。

命令模式：端口配置模式。

缺省情况：默认不启动 IPv6 安全 RA 功能。

使用指南：必须全局启动安全 RA 功能后，在端口上的安全 RA 才能启动。关闭全局安全 RA 后，清除掉所有已配置的安全 RA 端口。

举例：端口上启动 ipv6 安全 RA。

Switch(Config-If-Ethernet1/2)#ipv6 security-ra enable

10.3 show ipv6 security-ra

命令：show ipv6 security-ra [interface <interface-list>]

功能：显示那些接口启动了 ipv6 安全 RA 功能。

参数：不输入参数则显示所有的非信任端口，输入参数则显示相应的非信任端口。

命令模式：特权和配置模式。

举例：

Switch#show ipv6 security-ra

IPv6 security ra config and state information in the switch

Globe IPv6 Security RA State:Enable

Ethernet1/1
IPv6 Security RA State: Yes
Ethernet1/3
IPv6 Security RA State: Yes

10.4 debug ipv6 security-ra

命令：debug ipv6 security-ra
no debug ipv6 security-ra

功能：打开 IPv6 安全 RA 的调试信息；本命令的 no 操作为关闭 IPv6 安全 RA 的调试信息。

命令模式：特权配置模式。

参数：无。

使用指南：可以查看 IPv6 安全 RA 的报文接收转发处理，在遇到故障时有助于监测故障原因。

举例：打开 IPv6 安全 RA 的调试信息。

Switch#debug ipv security-ra

第 11 章 VLAN-ACL 配置命令

11.1 clear vACL statistic vlan

命令：clear vACL [in | out] statistic vlan [<1-4094>]

功能：此命令可清除 VACL 的统计信息。

参数：in | out: 清除入口/出口流量统计。

vlan <1-4094>：需要清除 VACL 统计信息的 VLAN，如果不输入 VLAN ID，则清除所有 VLAN 的统计信息。

命令模式：特权模式。

缺省情况：无。

使用指南：无。

举例：

清除 Vlan1 的 VACL 统计信息：

```
Switch# clear vACL statistic vlan 1
```

11.2 show vACL vlan

命令：show vACL [in | out] vlan [<1-4094>] | [begin | include | exclude <regular-expression>]

功能：此命令显示 VACL 的配置及统计信息。

参数：in | out: 显示入口/出口配置及统计。

vlan <1-4094>：需要显示 VACL 配置及统计信息的 VLAN，如果不输入 VLAN ID，则显示所有 VLAN 的 VACL 配置及统计信息。

begin | include | exclude <regular-expression>：正则表达式

· 匹配除换行符以外的任意字符

^ 匹配行的开始

\$ 匹配行的结束

| 匹配竖线左侧或右侧的字符串

[0-9] 匹配数字 0 到 9

[a-z] 匹配小写字母 a 到 z

[aeiou] 匹配 aeiou 中的任意一个字母

\ 转义字符，用于匹配元字符，例如\\$将匹配字符\$，而不是匹配字符串的结束

\w 匹配字母或数字或下划线

\b 匹配单词的开始或结束

\W 匹配任意不是字母，数字，下划线的字符

\B 匹配不是单词开头或结束的位置

[^x] 匹配除了 x 以外的任意字符

[^aeiou] 匹配除了 aeiou 这几个字母以外的任意字符

* 重复零次或更多次

+ 重复一次或更多次

{n} 重复 n 次
 {n,} 重复 n 次或更多次
 {n,m} 重复 n 到 m 次

目前使用的正则表达式不支持以下语法：

\s 匹配任意的空白符
 \d 匹配数字
 \S 匹配任意不是空白符的字符
 \D 匹配任意非数字的字符
 ? 重复零次或一次

命令模式：特权模式。

缺省情况：无。

使用指南：无。

举例：

Switch (config)#show vacl in vlan 2

Vlan 2:

IP Ingress access-list used is 100, traffic-statistics Disable.

Switch (config)# show vacl in vlan 3

Vlan 3:

IP Ingress access-list used is myacl, packet(s) number is 5.

显示信息	解释
Vlan 2	VLAN 名称
100、myacl	VACL 的名字
traffic-statistics Disable	VACL 统计功能关闭
packet(s) number is 5	匹配此 VACL 的 out-profile 数据报文总数

11.3 vacl ip access-group

命令：vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD
 no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD

功能：此命令在指定 VLAN 上配置 IP 类型的 VACL。

参数：<1-299> | WORD：可配置数字 IP ACL（包括：标准访问列表规则 <1-99>，扩展访问列表规则 <100-299>）或命名 ACL。

in | out：过滤入口\出口流量。

traffic-statistic：开启 VACL 匹配报文数统计功能。

vlan WORD：要绑定 VACL 的 VLAN。

命令模式：全局配置模式。

缺省情况：无。

使用指南：可以用“；”或“-”来输入或多个 VLAN，但最多不超过 128 个，并且 CLI 长度小于 80 个字符。目前在 VLAN Egress 方向上绑定 IP ACL 时不支持绑定匹配 tcp/udp range 的 ACL。

举例：为 Vlan1-5, 6, 7-9 配置数字 IP ACL，并开启统计功能。

Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9

11.4 vacl ipv6 access-group

命令：vacl ipv6 access-group (<500-699> | WORD) {in | out } (traffic-statistic|) vlan WORD

no ipv6 access-group {<500-699> | WORD} {in| out } vlan WORD

功能：此命令在指定 VLAN 上配置 IPv6 类型的 VACL。

参数：<500-699> | **WORD**：可配置数字 IP ACL（包括:IPv6 标准访问列表规则 <500-599>，IPv6 扩展访问列表规则 <600-699>）或命名 ACL。

in| out：过滤入口/出口流量。

traffic-statistic：开启 VACL 匹配报文数统计功能。

vlan WORD：要绑定 VACL 的 VLAN。

命令模式：全局配置模式。

缺省情况：无。

使用指南：可以用“;”或“-”来输入或多个 VLAN，但最多不超过 128 个，并且 CLI 长度小于 80 个字符。目前在 VLAN Egress 方向上绑定 IPv6 ACL 时不支持绑定匹配 flowlabel 的 ACL。

举例：为 Vlan5 配置数字 IPv6 ACL。

Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5

11.5 vacl mac access-group

命令：vacl mac access-group {<700-1199> | WORD} {in | out } [traffic-statistic] vlan WORD

no vacl mac access-group {<700-1199> | WORD} {in | out } vlan WORD

功能：此命令在指定 VLAN 上配置 MAC 类型的 VACL。

参数：<700-1199> | **WORD**：可配置数字 IP ACL（包括:<700-799> MAC 标准访问列表，<1100-1199> MAC 扩展访问列表）或命名 ACL。

in | out：过滤入口/出口流量。

traffic-statistic：开启 VACL 匹配报文数统计功能。

vlan WORD：要绑定 VACL 的 VLAN。

命令模式：全局配置模式。

缺省情况：无。

使用指南：可以用“;”或“-”来输入或多个 vlan，但最多不超过 128 个，并且 CLI 长度小于 80 个字符。

举例：为 Vlan1-5 配置数字 MAC ACL。

Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5

11.6 vacl mac-ip access-group

命令：vacl mac-ip access-group {<3100-3299> | WORD} {in | out } [traffic-statistic] vlan WORD

no vACL mac-ip access-group {<3100-3299> | WORD} {in | out } vlan WORD

功能：此命令在指定 VLAN 上配置 MAC-IP 类型的 VACL。

参数：<3100-3299>| WORD：可配置数字 IP ACL 或命名 ACL。

in | out：过滤入口/出口流量。

traffic-statistic：开启 VACL 匹配报文数统计功能。

vlan WORD：要绑定 VACL 的 VLAN。

命令模式：全局配置模式。

缺省情况：无。

使用指南：可以用“；”或“-”来输入或多个 VLAN，但最多不超过 128 个，并且 CLI 长度小于 80 个字符。目前在 VLAN Egress 方向上绑定 MAC-IP ACL 时不支持绑定匹配 tcp/udp range 的 ACL。

举例：为 Vlan1、2、5 配置数字 MAC-IP ACL。

Switch(config)#vACL mac-ip access-group 3100 in traffic-statistic vlan 1;2;5

第 12 章 SAVI 配置命令

12.1 SAVI 配置命令

12.1.1 ipv6 cps prefix

命令：ipv6 cps prefix <ipv6-address> vlan <vid>

no ipv6 cps prefix <ipv6-address>

功能：手工配置链路 IPv6 地址前缀，本命令的 no 操作为删除链路 IPv6 地址前缀。

参数：ipv6-address: 为链路前缀地址，如 2001::/64;

vid: 当前链路所属 vlan ID。

命令模式：全局配置模式。

缺省情况：无。

使用指南：若用户启用匹配链路地址前缀功能，请首先配置链路本地地址前缀：fe80::/64，以放行所有源地址为链路本地地址的报文。

举例：配置 2001::/64 的链路前缀地址。

Switch(config)#ipv6 cps prefix 2001::/64

12.1.2 ipv6 cps prefix check enable

命令：ipv6 cps prefix check enable

no ipv6 cps prefix check enable

功能：使能 SAVI 地址前缀检查功能；本命令的 no 操作为关闭 SAVI 地址前缀检查功能。

参数：无。

命令模式：全局配置模式。

缺省情况：关闭 SAVI 地址前缀检查功能。

使用指南：使能前缀检查功能后，对嗅探报文的 IPv6 地址进行前缀匹配检查，若不符合当前链路前缀，则不建立对应的 IPv6 地址绑定；若用户启用匹配链路地址前缀功能，请首先配置链路本地地址前缀：fe80::/64，以放行所有源地址为链路本地地址的报文。默认关闭地址前缀检查功能。

举例：使能 SAVI 地址前缀检查功能。

Switch(config)#ipv6 cps prefix check enable

12.1.3 ipv6 dhcp snooping trust

命令：ipv6 dhcp snooping trust

no ipv6 dhcp snooping trust

功能：配置该端口为 dhcpv6 trust 端口功能，该端口不再建立 DHCPv6 类型的动态绑定，放行所有 DHCPv6 协议报文；no 命令为删除端口 trust 功能。

参数：无。

命令模式：端口配置模式。

缺省情况：默认关闭端口信任功能。

使用指南：设置该端口为 dhcpv6 trust 属性，一般开启 SAVI 功能交换机的连接 dhcpv6 server 或 dhcpv6 relay 的上联端口。

举例：设置端口 ethernet1/1 为 DHCP 信任端口。

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

```
Switch(config-if-ethernet1/1)#ipv6 dhcp snooping trust
```

12.1.4 ipv6 nd snooping trust

命令：ipv6 nd snooping trust

no ipv6 nd snooping trust

功能：配置该端口为 slaac trust 和 RA trust 端口，该端口不再建立 slaac 类型的动态绑定，并且转发 RA 报文；no 命令为删除端口 trust 功能。

参数：无。

命令模式：端口配置模式。

缺省情况：默认关闭端口信任功能。

使用指南：如果端口没有启用 ipv6 nd snooping trust 功能，则该端口被认为非信任 RA 报文端口，丢弃收到的所有 RA 报文，设置该端口为 trust 属性，一般为开启 SAVI 交换机功能的上联路由器端口，或开启 SAVI 交换机之间的互联端口。

举例：设置端口 ethernet1/1 为 nd 信任端口。

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

```
Switch(config-if-ethernet1/1)#ipv6 nd snooping trust
```

12.1.5 savi check binding

命令：savi check binding <simple | probe> mode

no savi check binding mode

功能：配置冲突绑定的检查模式；本命令的 no 操作为删除冲突绑定的检查模式。

参数：simple 模式：只检查冲突绑定端口所处的状态，若冲突绑定所在端口为 up 状态，则维持冲突绑定，不建立新绑定；若冲突绑定所在端口为 down 状态，则删除冲突绑定，建立新绑定；

probe 模式：除检查冲突绑定的所在端口状态外，若冲突绑定所在端口为 up 状态，还要发出 NS 报文去探测冲突绑定对应用户的可用性，若收到用户端回应的 NA 报文，则维持原冲突绑定，不建立新绑定，否则删除原冲突绑定，建立新绑定。

命令模式：全局配置模式。

缺省情况：默认为关闭冲突绑定检查模式，采取直接删除冲突绑定，创建新绑定的方式。

使用指南：建议用户配置 probe 模式，防止伪造的地址绑定冲突删除合法用户绑定的攻击。

举例：设置冲突绑定的检查模式为 probe 模式。

```
Switch(config)#savi check binding probe mode
```

12.1.6 savi enable

命令： savi enable

no savi enable

功能： 打开全局 SAVI 功能；本命令的 no 操作为关闭全局 SAVI 功能。

参数： 无。

命令模式： 全局配置模式。

缺省情况： 默认关闭 SAVI 全局功能。

使用指南： 使能 SAVI 全局功能后，才能进行 SAVI 功能的命令配置，SAVI 功能已经包含了安全 RA 功能，在全局配置上，SAVI 全局功能与安全 RA 全局功能互斥。

举例： 使能 SAVI 功能。

Switch(config)#savi enable

12.1.7 savi ipv6 binding num

命令： savi ipv6 binding num <limit-num>

no savi ipv6 binding num

功能： 配置端口对应的绑定数目，no 命令为还原默认值。

参数： limit-num：设置范围为 0-65535 个，端口绑定数目默认值为 65535 个。

命令模式： 端口配置模式。

缺省情况： 默认值为 65535 个。

使用指南： 该绑定配置数目仅包括 slaac, dhcp 类型的动态绑定，若绑定总数超过该配置数目，则该端口不再创建任何新的动态绑定，若配置数目为 0，则该端口不建立任何动态绑定。

举例： 设置端口 ethernet1/1 的绑定数目为 100。

Switch(config)#interface ethernet1/1

Switch(config-if-ethernet1/1)#savi ipv6 binding num 100

12.1.8 savi ipv6 check source binding

命令： savi ipv6 check source binding ip <ip-address> mac <mac-address> interface <if-name> {type [slaac | dhcp] lifetime <lifetime> | type static}

no savi ipv6 check source binding ip <ip-address> interface <if-name>

功能： 手工配置动态或静态绑定功能；本命令的 no 操作为删除手工配置的动态或静态绑定功能。

参数： ip-address：为 IPv6 单播地址，包括本地链路和全球单播地址；

mac-address：为以太网 mac 地址；

if-name：为端口名，如 interface ethernet 1/1；

slaac | dhcp：slaac 表示创建 slaac 类型动态绑定，dhcp 表示创建 dhcp 类型动态绑定；

lifetime：配置动态绑定的生存周期，单位为秒；

static：创建静态类型绑定。

命令模式： 全局配置模式。

缺省情况： 无。

使用指南： 手工配置的动态绑定超时后，会删除该配置对应的绑定，但配置仍保留，因此显示绑定信息时仍会显示该绑定信息；若让该配置对应的绑定重新生效，则需先删除，然后进

行重新配置。

绑定类型为 **static** 类型，则无需配置绑定生存周期，生存周期为 **infinite**。

举例：

手工配置 SAVI slaac 类型动态绑定。

```
Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04
Interface ethernet1/1 type slaac lifetime 2010
```

手工配置 SAVI 静态类型绑定。

```
Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04
Interface ethernet1/1 type static
```

12.1.9 savi ipv6 check source ip-address mac-address

命令： **savi ipv6 check source [ip-address mac-address | ip-address | mac-address]**
no savi ipv6 check source

功能： 使能端口报文控制验证功能；no 命令为关闭端口报文控制验证功能。

参数： 无。

命令模式： 端口配置模式。

缺省情况： 默认关闭报文控制过滤功能。

使用指南： 必须使能 SAVI 全局功能后，才能配置该命令。

举例： 在端口 **ethernet1/1** 时，使能报文控制过滤功能。

```
Switch(config)#interface ethernet1/1
Switch(config-if-ethernet1/1)#savi ipv6 check source ip-address mac-address
```

12.1.10 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac}

enable

命令： **savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable**
no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

功能： 使能 SAVI 应用场景功能；本命令的 no 操作为关闭 SAVI 应用场景功能。

参数： dhcp-only: dhcp-only 应用场景

slaac-only: slaac-only 应用场景

dhcp-slaac: dhcp-only 与 slaac-only 组合应用场景

命令模式： 全局配置模式。

缺省情况： 关闭 SAVI 应用场景。

使用指南： dhcp-only 应用场景仅嗅探 DHCPv6 报文和 target 字段 IPv6 地址为 link-local ipv6 地址的 DAD NS 报文，对非 link-local 地址 DAD NS 报文不进行嗅探；而 slaac-only 应用场景则嗅探所有类型的 DAD NS 报文；dhcp-slaac 组合应用场景则嗅探所有的 DHCPv6 和 DAD NS 报文；默认为关闭 SAVI 各种应用场景嗅探功能。

举例： 使能 SAVI dhcp-only 特定应用场景。

```
Switch(config)#savi ipv6 dhcp-only enable
```

12.1.11 savi ipv6 mac-binding-limit

命令: **savi ipv6 mac-binding-limit <limit-num>**

no savi ipv6 mac-binding-limit

功能: 配置同一 MAC 地址对应的动态绑定数目; no 命令为恢复默认值。

参数: limit-num: 设置范围 1-10, 同一 MAC 地址对应的默认动态绑定数目为 32 个。

命令模式: 全局配置模式。

缺省情况: 默认值为 32 个。

使用指南: 该命令主要用于防止 SAVI 动态绑定表项的耗尽攻击。

举例: 设置同一 MAC 地址对应的动态绑定数为 5。

Switch(config)#savi ipv6 mac-binding-limit 5

12.1.12 savi max-dad-delay

命令: **savi max-dad-delay <max-dad-delay>**

no savi max-dad-delay

功能: 配置动态绑定处于 DETECTION 状态, 发出 DAD NS 报文探测的生存周期, no 命令为恢复默认值。

参数: max-dad-delay: 设置范围为 1-65535 秒, max-dad-delay 默认值为 1 秒。

命令模式: 端口配置模式。

缺省情况: 采用默认值 1 秒。

使用指南: 建议用户采用默认值 1 秒。

举例: 设置探测生存期为 2 秒。

Switch(config)#savi max-dad-delay 2

12.1.13 savi max-dad-prepare-delay

命令: **savi max-dad-prepare-delay <max-dad-prepare-delay>**

no savi max-dad-prepare-delay

功能: 配置动态绑定重新探测的生存周期, no 命令为恢复默认值。

参数: max-dad-prepare-delay: 设置范围为 1-65535 秒, max-dad-prepare-delay 默认值为 1 秒。

命令模式: 全局配置模式。

缺省情况: 默认值为 1 秒。

使用指南: 建议用户采用默认值 1 秒。

举例: 设置重新探测生存期为 2 秒。

Switch(config)#savi max-dad-prepare-delay 2

12.1.14 savi max-slaac-life

命令: **savi max-slaac-life <max-slaac-life>**

no savi max-slaac-life

功能：配置 slaac 动态绑定处于 BOUND 状态的生存周期，no 命令为恢复默认值。

参数：max-slaac-life：设置范围 1-31536000 秒，max-slaac-life 默认为 4 小时。

命令模式：全局配置模式。

缺省情况：默认值为 4 小时。

使用指南：无。

举例：设置 slaac 类型绑定的 BOUND 状态的生存周期为 2010 秒。

Switch(config)#savi max-slaac-life 2010

12.1.15 savi timeout bind-protect

命令：savi timeout bind-protect <protect-time>

no savi timeout bind-protect

功能：配置端口由 up 状态变成 down 状态后，对该端口绑定进行保护的生存周期；no 命令为恢复默认值。

参数：protect-time：设置范围 1-300 秒，protect-time 默认为 30 秒。

命令模式：全局配置模式。

缺省情况：默认值为 30 秒。

使用指南：若配置生存周期超时后，端口仍处于 down 状态，则将删除该端口上的绑定；若在配置生存周期内，端口由 down 状态转为 up 状态，则该端口上的绑定将重新设置其生存周期为 BOUND 状态的生存周期。若配置参数为 0 秒，则立即删除端口上的所有绑定。

举例：设置保护绑定的生存周期为 20 秒。

Switch(config)#savi timeout bind-protect 20

12.2 SAVI 监控和调试命令

12.2.1 监控和调试信息

12.2.1.1 debug ipv6 dhcp snooping binding

命令：debug ipv6 dhcp snooping binding

no debug ipv6 dhcp snooping binding

功能：打开 SAVI dhcp 类型绑定调试信息开关；本命令的 no 操作为关闭 SAVI dhcp 类型绑定调试信息开关。

参数：无。

命令模式：特权用户模式。

缺省情况：无。

使用指南：当打开该调试开关后，将会有相关 SAVI dhcp 类型以及静态类型绑定创建删除打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

举例：打开 dhcp 类型绑定调试信息开关。

Switch#debug ipv6 dhcp snooping binding

12.2.1.2 debug ipv6 dhcp snooping event

命令：debug ipv6 dhcp snooping event
no debug ipv6 dhcp snooping event

功能：打开 SAVI dhcp 类型事件调试信息开关；本命令的 no 操作为关闭 SAVI dhcp 类型事件调试信息开关。

参数：无。

命令模式：特权用户模式。

缺省情况：无。

使用指南：当打开该事件开关后，将会有相关 dhcp 类型事件打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

举例：打开 DHCP 类型绑定事件调试信息开关。

Switch#debug ipv6 dhcp snooping event

12.2.1.3 debug ipv6 dhcp snooping packet

命令：debug ipv6 dhcp snooping packet
no debug ipv6 dhcp snooping packet

功能：打开 DHCPv6 报文调试信息开关；本命令的 no 操作为关闭 DHCPv6 报文调试信息开关。

参数：无。

命令模式：特权用户模式。

缺省情况：无。

使用指南：当打开该报文调试开关后，将会有相关 DHCPv6 报文打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

举例：打开 DHCPv6 报文调试信息开关。

Switch#debug ipv6 dhcp snooping packet

12.2.1.4 debug ipv6 nd snooping binding

命令：debug ipv6 nd snooping binding
no debug ipv6 nd snooping binding

功能：打开 SAVI slaac 类型绑定调试信息开关；本命令的 no 操作为关闭 SAVI slaac 类型绑定调试信息开关。

参数：无。

命令模式：特权用户模式。

缺省情况：无。

使用指南：当打开该调试开关后，将会有相关 SAVI slaac 类型绑定创建删除打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

举例：打开 slaac 类型绑定调试信息开关。

Switch#debug ipv6 nd snooping binding

12.2.1.5 debug ipv6 nd snooping event

命令：debug ipv6 nd snooping event
no debug ipv6 nd snooping event

功能：打开 SAVI slaac 类型事件调试信息开关；本命令的 no 操作关闭 SAVI slaac 类型事件调试信息开关。

参数：无。

命令模式：特权用户模式。

缺省情况：无。

使用指南：当打开该事件开关后，将会有相关 slaac 类型事件打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

举例：打开 slaac 类型事件调试信息开关。

Switch#debug ipv6 nd snooping event

12.2.1.6 debug ipv6 nd snooping packet

命令：debug ipv6 nd snooping packet

no debug ipv6 nd snooping packet

功能：打开 ND 报文调试信息开关；本命令的 no 操作为关闭 ND 报文调试信息开关。

参数：无。

命令模式：特权用户模式。

缺省情况：无。

使用指南：当打开该报文调试开关后，将会有相关 ND 报文打印信息，便于在出错时进行排错。使用 no 命令可关闭该排错功能。

举例：打开 ND 报文调试信息开关。

Switch#debug ipv6 nd snooping packet

12.2.1.7 show savi ipv6 check source binding

命令：show savi ipv6 check source binding [interface <if-name>]

功能：显示全局 SAVI 绑定表项。

参数：if-name: 为端口名，如 interface ethernet 1/1。

命令模式：特权用户模式。

缺省情况：无。

使用指南：各显示字段含义如下表

字段	描述
MAC	绑定的 MAC 地址
IP	绑定的 IP 地址
Vlan	绑定所属 Vlan
Port	绑定所属端口
Type	绑定类型
State	绑定状态
Expires	绑定的生存周期

举例：显示 SAVI 全局绑定状态。

Switch(config)#show savi ipv6 check source binding

Static binding count: 0

Dynamic binding count: 3

Binding count: 3

MAC	IP	VLAN	Port	Type	State	Expires
00-25-64-bb-8f-04	fe80::225:64ff:febb:8f04	1	Ethernet1/5	slaac	BOUND	14370
00-25-64-bb-8f-04	2001::13	1	Ethernet1/5	slaac	BOUND	14370
00-25-64-bb-8f-04	2001::10	1	Ethernet1/5	slaac	BOUND	14370

第 13 章 Captive Portal 认证命令

13.1 认证功能命令

13.1.1 ac-name

命令：ac-name <word>

no ac-name

功能：配置重定向 url 中的参数 acname 的值。本命令的 no 形式为删除重定向 url 中的参数 acname 值的配置。

参数：<word>，为 acname 的值。最多 16 个字符。

命令模式：Captive Portal Instance 模式。

缺省情况：无。

使用指南：本命令用于配置重定向 url 中的参数 acname 的值。某些 portal server 要求重定向时带上特定的 ac-name 值才能够通过认证，所以需要根据 portal server 的要求来配置此命令。

举例：根据移动 portal server 的标准配置重定向 url 中的 ac-name 值为 0100.0010.010.00，命名格式为 ACN.CTY.PRO.OPE。

Switch(config-cp-instance)#ac-name 0100.0010.010.00

13.1.2 authentication roam enable

命令：authentication roam enable <vlan WORD>

no authentication roam enable <vlan WORD>

功能：使能用户漫游功能。该命令的 no 操作为关闭用户漫游功能。

参数：vlan WORD：指定的 VLAN 允许漫游。

命令模式：captive portal 配置模式。

缺省情况：默认不开启。

使用指南：使能该功能后，则允许用户漫游。当一个用户从一个端口漫游到另外一个端口时（同一个 VLAN），就可以触发漫游，用户不需要重新认证就可以访问网络资源；关闭用户漫游功能，不允许用户漫游。当一个用户从一个端口漫游到另外一个端口时，需要重新认证才可以访问网络资源。

举例：vlan10 开启用户漫游。

Switch (config-cp)#authentication roam enable vlan 10

13.1.3 captive-portal

命令：captive-portal

功能：使用该命令进入 Captive Portal 配置模式。

参数：无。

缺省情况：无。

命令模式：全局配置模式。

使用指南：使用该命令进入 Captive Portal 配置模式。

举例：进入全局配置模式进行相应配置。

Switch (config)#captive-portal

13.1.4 captive-portal binding arp（暂不支持）

命令： **captive-portal binding arp**

no captive-portal binding arp

功能：使能绑定静态 arp 功能后，用户认证成功后，为用户绑定一条静态 arp，用户下线后，删除绑定的静态 arp。该命令的 no 操作为删除所有绑定的静态 ARP，用户上线后，不再绑定静态 ARP。

参数：无。

缺省情况：无。

命令模式：captive portal 模式。

使用指南：使用该命令进入 Captive Portal 配置模式。

举例：进入 captive portal 配置模式进行相应配置。

Switch (config)# captive-portal binding arp

13.1.5 captive-portal client deauthenticate

命令： **captive-portal client deauthenticate {<1-10> | <FF-FF-FF-FF-FF-FF> { ipv4 | ipv6} <ip-addr>}**

功能：该命令解关联特定的 Captive Portal 客户端。

参数：<1-10> Captive Portal 的 ID；

<FF-FF-FF-FF-FF-FF>客户端的 MAC 地址；

ipv4 用户地址为 ipv4 地址；

ipv6 用户地址为 ipv6 地址；

<ip-addr>用户地址，ipv4 地址是以点分十进制格式，ipv6 地址是 X:X::X:X 的格式。

缺省情况：无。

命令模式：特权模式。

使用指南：使用此命令可以解关联指定 MAC 地址的客户端；也可解除指定 captive portal configuration 下的所用用户或单独用户；当没有参数时，将解除所有用户。

举例：解关联特定的 Captive Portal 客户端。

Switch #captive-portal client deauthenticate （强制该控制器上所有的 portal 用户下线）

The specified clients will be deauthenticated. Are you sure you want to deauthenticated clients? [Y/N]

Switch #captive-portal client deauthenticate 1（强制例程 1 上所有的用户下线）

Switch #captive-portal client deauthenticate 34-08-04-30-07-ca ipv4 100.1.1.1（强制某个用户下线）

13.1.6 captive-portal client re-auth log { enable | disable }

命令：captive-portal client re-auth log enable
captive-portal client re-auth log disable

功能：当用户上来的端口，vlan，mac 发生改变，需要重新认证时，show logging buffer 里会记录日志。该命令的 no 操作为重新认证时，不记录日志。

参数：无。

缺省情况：默认不开启。

命令模式：captive portal 模式。

使用指南：当在线用户认证的端口,或者 vlan，或者 mac 发生改变，需重新认证时，记录日志。

举例：Switch (config-cp)# captive-portal client re-auth log enable

13.1.7 captive-portal client keep-alive flow-detection enable

命令：captive-portal client keep-alive flow-detection enable
no captive-portal client keep-alive flow-detection enable

功能：使能用户保活功能。该命令的 no 操作为关闭用户保活功能。

参数：无。

缺省情况：默认不开启。

命令模式：captive portal 模式。

使用指南：使能该功能后，当用户上线后，对用户进行保活。

举例：进入 captive portal 配置模式进行相应配置。

Switch (config-cp)#captive-portal client keep-alive flow-detection enable

13.1.8 captive-portal client keep-alive flow-detection interval

命令：captive-portal client keep-alive flow-detection interval <3-120>
no captive-portal client keep-alive flow-detection interval

功能：设定用户保活查询间隔。该命令的 no 操作，为设置保活查询间隔为默认值。

参数：<3-120>参数范围为 3 分钟到 120 分钟。

缺省情况：默认为 5 分钟。

命令模式：captive portal 模式。

使用指南：配置该命令后，保活定时器每隔设定时间查询一次用户在线状态。

举例：进入 captive portal 配置模式进行相应配置。

Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

13.1.9 captive-portal client keep-alive flow-detection number

命令：captive-portal client keep-alive flow-detection number <1-10>

no captive-portal client keep-alive flow-detection number

功能：设置允许保活定时器连续查询失败次数。该命令的 no 操作为设置允许保活定时器连续查询失败次数为默认值。

参数：<1-10>:范围 1 次到 10 次。

缺省情况：默认是 3 次。

命令模式：captive portal 模式。

使用指南：配置该命令后，保活定时器连续查询指定次数用户在线状态，如都不在线，则认为用户下线，否则，只要在允许失败次数内有 1 次查到用户在线，认为用户还在线，重置已经查询失败计数。

举例：进入 captive portal 配置模式进行相应配置。

Switch (config-cp)# captive-portal client keep-alive flow-detection interval 3

13.1.10 clear

命令：clear

功能：该命令设置例程的配置到默认值。

参数：无。

缺省情况：无。

命令模式：Captive Portal Instance 配置模式。

使用指南：设置 portal 例程的配置到默认值。

举例：设置例程的配置到默认值。

Switch (config-cp-instance)# clear

13.1.11 configuration

命令：configuration <cp-id>

no configuration <cp-id>

功能：使用该命令进入 Captive Portal 例程模式。该命令的 no 操作为删除 Captive Portal 例程配置。

参数：<cp-id>为 Captive Portal 例程数量，取值范围为 1-10。

缺省情况：无。

命令模式：Captive Portal 全局配置模式。

使用指南：该配置用于配置 Captive Portal 的例程，每一个例程代表一类场景，处于同一例程下的用户其流量、速率等配置相同，反之亦然。该命令的 no 模式删除一个 captive portal 配置。如果有接口关联在某个例程上，则对该例程使用 no 命令无效。

举例：配置 ID 参数为 4。

Switch (config-cp)#configuration 4

13.1.12 debug captive-portal packet

命令：debug captive-portal packet {send|receive|all}
no debug captive-portal packet {send|receive|all}

功能：打开 captive portal 认证功能的报文调试开关。本命令的 no 形式为关闭 captive portal 认证功能的报文调试开关。

参数：send，为打开 captive portal 的发包调试信息；
receive，为打开 captive portal 的收包调试信息；
all，为打开 captive portal 的收发包和解析包调试信息。

命令模式：特权模式。

缺省情况：缺省情况下 captive portal 认证功能的报文调试信息是关闭的。

使用指南：本命令用于打开 captive portal 认证功能的报文调试开关。

举例：打开 captive portal 认证功能的收发包和解析包调试信息。

Switch #debug captive-portal packet all

13.1.13 debug captive-portal trace

命令：debug captive-portal trace
no debug captive-portal trace

功能：打开 captive portal 认证功能的跟踪情况调试。本命令的 no 形式为关闭 captive portal 认证功能的跟踪情况调试。

参数：无。

命令模式：特权模式。

缺省情况：缺省情况下 captive portal 认证功能的跟踪调试是关闭的。

使用指南：本命令用于打开 captive portal 认证功能的跟踪情况调试。

举例：打开 captive portal 认证功能的跟踪情况调试。

Switch #debug captive-portal trace

13.1.14 debug captive-portal alive-detail

命令：debug captive-portal alive-detail
no debug captive-portal alive-detail

功能：portal 认证保活处理详细调试信息。

参数：无。

缺省情况：无。

命令模式：特权用户配置模式。

举例：Switch#debug captive-portal alive-detail

13.1.15 debug captive-portal alive-status

命令：debug captive-portal alive-status
no debug captive-portal alive-status

功能: portal 认证保活处理状态调试信息。

参数: 无。

缺省情况: 无。

命令模式: 特权用户配置模式。

举例: Switch#debug captive-portal alive-status

13.1.16 debug captive-portal alive-time

命令: **debug captive-portal alive-time**

no debug captive-portal alive-time

功能: portal 认证保活处理时间调试信息。

参数: 无。

缺省情况: 无。

命令模式: 特权用户配置模式。

举例: Switch#debug captive-portal alive-time

13.1.17 debug captive-portal error

命令: **debug captive-portal error**

no debug captive-portal error

功能: 打开 captive portal 认证功能的错误调试信息。本命令的 no 形式为关闭 captive portal 认证功能的错误调试信息。

参数: 无。

命令模式: 特权模式。

缺省情况: 缺省情况下 captive portal 认证功能的错误调试信息是关闭的。

使用指南: 本命令用于打开 captive portal 认证功能的错误调试信息。

举例: 打开 captive portal 认证功能的错误调试信息。

Switch #debug captive-portal error

13.1.18 enable (全局)

命令: **enable**

disable

功能: 使用 enable 命令全局使能控制器上的 Captive Portal 功能, 使用 disable 功能全局关闭控制器上的 Captive Portal 功能。

参数: 无。

缺省情况: 全局关闭控制器上的 Captive Portal 功能。

命令模式: Captive Portal 全局配置模式

使用指南: 使用该命令全局使能 Captive Portal 在控制器上的特征。

举例: 打开 Captive Portal 在控制器上的全局功能。

Switch (config-cp)#enable

13.1.19 enable (例程)

命令: **enable**

disable

功能: 该命令使能 Captive Portal 配置。

参数: 无。

缺省情况: 使能 Captive Portal 配置。

命令模式: Captive Portal Instance 配置模式

使用指南: 默认为 enable 模式, 关闭 captive-portal 功能的命令为 disable, 关闭 portal 功能后在线的 portal 用户被强制下线。

举例: 打开 captive-portal 功能。

Switch (config-cp-instance)#enable

13.1.20 external portal-server server-name

命令: **external portal-server server-name <name> {ipv4 | ipv6} <ipaddr> [port <1-65535>]**

no external portal-server {ipv4 | ipv6}server-name <name>

功能: 该命令配置外置 portal 服务器, 通过该服务器推出重定向页面, 客户端输入正确的用户名和密码后, 认证成功, 该客户端能够访问外网。

参数: <name> 外置 portal 服务器的名字

<ipaddr> 外置 portal 服务器的 ip 地址

ipv4 配置的 Portal 服务器地址是 ipv4 地址

ipv6 配置的 Portal 服务器地址是 ipv6 地址

<1-65535> portal server 的端口号

缺省情况: 无。

命令模式: Captive Portal 全局配置模式

使用指南: 配置外置 portal 服务器, 最多可以配置 10 台。每个 cp configuration 可以绑定一台 portal 服务器。

举例: 配置一个外置 portal 服务器。

Switch (config-cp)# external portal-server server-name x1 ipv4 1.0.0.1 port 11111

13.1.21 http-redirect-filter <1-32> {ip A.B.C.D| domain WORD}

命令: **http-redirect-filter <1-32> {ip A.B.C.D| domain WORD}**

no http-redirect-filter (<1-32>|all)

功能: 为 portal 认证的 HTTP 重定向指定 IP 或域名, 只有匹配了这个 IP 或域名的 HTTP 报文才做重定向处理。no 操作为删除配置认证域名或 ip 地址后, 按照之前的流程认证, 所有未认证的 mac, 认证前 http 报文均重定向到 portal server。

参数: <1-32> : 规则 ID 号 (索引);

ip A.B.C.D: HTTP 重定向指定 IP 地址;

domain WORD: HTTP 重定向指定域名, 最大长度为 256。

缺省情况: 默认不配置此命令, 所有未认证的 mac, 认证前 http 报文均重定向到 portal server。

命令模式: Captive Portal 配置模式。

使用指南: 增加一条配置认证域名或者 ip 地址的命令。

举例: 配置一条指定 ip 地址为 1.1.1.1 的命令。

Switch (config-cp)# http-redirect-filter 1 ip 1.1.1.1

配置一条指定域名为 www.dcn.com 的命令。

Switch (config-cp)# http-redirect-filter 1 domain www.dcn.com

13.1.22 http-redirect-filter <1-32>

命令: **http-redirect-filter <1-32>**

no http-redirect-filter <1-32>

功能: captive portal 的一个实例绑定一个规则。该命令的 no 操作是删除一个 redirect 绑定。

参数: **<1-32>**: 规则 ID 号 (索引)。

缺省情况: 默认不配置此命令。

命令模式: Captive Portal Instance 模式。

使用指南: captive portal 的一个实例进行一个 redirect 绑定。

举例: 实例绑定规则。

Switch (config-cp-instance)# http-redirect-filter 1

13.1.23 name

命令: **name <cp-name>**

no name

功能: 该命令定义 Captive Portal 配置的名称。

参数: **<cp-name>**, Captive Portal 配置的名称, 其最多可以包含 32 个字符的字母或数字。

缺省情况: 无。

命令模式: Captive Portal Instance 配置模式

使用指南: 定义 Captive Portal Instance 配置的名称。

举例: 定义 Captive Portal 配置的名称为 abc123。

Switch (config-cp-instance)#name abc123

13.1.24 nas-ipv4

命令: **nas-ipv4 <A.B.C.D>**

no nas-ipv4 <A.B.C.D>

功能: 该命令定义 Captive Portal nas-ip 地址。

参数: **<A.B.C.D>**, IPv4 address of NAS。

缺省情况: 无。

命令模式: Captive Portal 配置模式。

使用指南：定义 Captive Portal nas-ip 地址。

举例：配置 Captive Portal nas-ip 地址是 10.1.1.1。

Switch (config-cp)#nas-ip 10.1.1.1

13.1.25 portal enable configuration <id> [vlan-pool WORD]

命令：portal enable configuration <id> [vlan-pool WORD]

no portal enable [vlan-pool WORD]

功能：端口下使能 portal 功能，指定端口绑定的实例号，并且可以指定哪些 VLAN 使能 portal。一个端口只能绑定一个实例，可以绑多个 VLAN 池。

参数：<id>：指定实例号。

vlan-pool WORD：vlan 池，可以配多个。

缺省情况：无。

命令模式：端口配置模式。

使用指南：端口下使能 portal 功能，并且将端口绑定到某个实例，绑定后，实例下的规则可以应用到这个端口。对于不指定 VLAN 参数的情况，端口下所有 VLAN 的流量都要进行认证；指定 VLAN 的情况下，只有指定 VLAN 下的流量进行认证，其他 VLAN 的流量不进行认证（其他 VLAN 流量放行）。

端口下关闭 portal 功能，对于不带 VLAN 参数的情况，端口所有 VLAN 关闭 portal 认证，流量恢复正常；指定 VLAN 的情况下，基于 VLAN 关闭 portal 认证，端口下指定 VLAN 的流量恢复正常（VLAN 流量放行）。

举例：配置端口 1/1 下绑定 configuration 1 的实例和 vlan 3。

Switch (config-if-ethernet1/1)#portal enable configuration 1 vlan-pool 3

13.1.26 portal-server

命令：portal-server {ipv4 | ipv6} <name>

no portal-server {ipv4 | ipv6}

功能：该命令为 CP configuration 配置绑定特定的外置 portal 服务器。绑定到此 CP configuration 下的端口都通过这个 portal 服务器进行重定向认证。

参数：<name> 绑定的 Portal 服务器的名字

ipv4 绑定的 Portal 服务器地址是 ipv4 地址

ipv6 绑定的 Portal 服务器地址是 ipv6 地址

缺省情况：无。

命令模式：Captive Portal Instance 配置模式

使用指南：使用此命令可以为 CP configuration 配置绑定特定的外置 portal 服务器；也可 configuration 解除绑定特定的外置 portal 服务器。

举例：为 CP configuration 配置绑定特定的外置 portal 服务器。

Switch (config-cp -instance)#portal-server ipv4 x1

13.1.27 radius accounting

命令：radius accounting

no radius accounting

功能：使用该命令打开 Captive Portal 例程的计费功能。该命令的 no 操作为关闭 Captive Portal 例程的计费功能

参数：无。

缺省情况：Captive Portal 例程的计费功能关闭。

命令模式：Captive Portal Instance 配置模式

使用指南：配置 Captive Portal 的计费功能。

举例：打开 Captive Portal 某例程的计费功能。

Switch (config-cp-instance)#radius accounting

13.1.28 radius-accounting update interval

命令：radius-accounting update interval <60-3600>

no radius-accounting update interval

功能：配置交换机向 radius 发送的 portal 用户的计费更新间隔时间。该命令的 no 操作为恢复配置的默认值。

参数：<60-3600>为时间间隔，单位为秒。

缺省情况：300 秒

命令模式：Captive Portal Instance 配置模式

使用指南：配置 Captive Portal 的计费更新间隔时间。

举例：配置交换机向 radius 发送的 portal 用户的计费更新间隔时间为 60 秒。

Switch (config-cp-instance)# radius-accounting update interval 60

13.1.29 radius-acct-server

命令：radius-acct-server <server-name>

no radius-acct-server

功能：使用该命令定义 Captive Portal 配置的 RADIUS 计费服务器名称。该命令的 no 操作为删除此次配置。

参数：<server-name>，RADIUS计费服务器名称

缺省情况：无。

命令模式：Captive Portal Instance 配置模式

使用指南：定义 Captive Portal 配置的 RADIUS 计费服务器。

举例：定义 Captive Portal 配置的 RADIUS 计费服务器为 radius_aaa_1。

Switch (config-cp-instance)#radius-acct-server radius_aaa_1

13.1.30 radius-auth-server

命令：radius-auth-server <server-name>

no radius-auth-server

功能：使用该命令定义 Captive Portal 配置的 RADIUS 认证服务器。该命令的 no 操作为删除此次配置。

参数： <server-name>，Captive Portal 配置的 RADIUS 认证服务器名称

缺省情况： 无。

命令模式： Captive Portal Instance 配置模式

使用指南： 定义 Captive Portal 配置的 RADIUS 认证服务器。

举例： 定义 Captive Portal 配置的 RADIUS 认证服务器为 radius_aaa_1。

Switch (config-cp-instance)#radius-auth-server radius_aaa_1

13.1.31 redirect url-head <word>

命令： redirect url-head <word>

no redirect url-head

功能： 配置重定向 url 头部分，包括传输协议、主机名、端口和 path 等几个部分。本命令的 no 形式为删除重定向 url 头部分的配置。

参数： <word>，重定向 url 头部分。如 https://200.101.13.4:8080/index.jsp。也可以为 http://www.portal.com/index.jsp。最多可输入 128 个字符。

命令模式： captive portal instance 配置模式。

缺省情况： 无。

使用指南： 本命令用于配置重定向 url 头部分，包括传输协议、主机名、端口和 path 等几个部分。需要根据 portal server 上重定向页面的 url 来配置，传输协议、主机名、端口和 path 需要完全相同才能进行重定向。

举例： 配置重定向 url 头部分为 http://17.16.1.26/control

Switch (config-cp-instance)#redirect url-head http://17.16.1.26/control

13.1.32 redirect attribute ssid enable

命令： redirect attribute ssid enable

no redirect attribute ssid enable

功能： 使能重定向 url 中携带 ssid 参数功能。本命令的 no 形式为关闭重定向 url 中携带 ssid 参数的功能。

参数： 无。

命令模式： captive portal instance 配置模式。

缺省情况： 缺省情况下重定向 url 中携带 ssid 参数的功能是关闭的。

使用指南： 本命令用于使能重定向 url 中携带 ssid 参数功能。使能此功能后，客户端进行重定向时，重定向的 url 中会携带客户端关联的 ssid。

举例： 使能重定向 url 中携带 ssid 参数功能。

Switch (config-cp-instance)#redirect attribute ssid enable

13.1.33 redirect attribute ssid name

命令： redirect attribute ssid name <word>

no redirect attribute ssid name

功能： 配置在重定向 url 中携带的 ssid 参数名称。本命令的 no 形式为恢复冲向 url 中携带的 ssid 参数名称为默认值。

参数：<word>，为 ssid 参数名称。最多 32 个字符

命令模式：captive portal instance 配置模式。

缺省情况：缺省情况下重定向 url 中携带的 ssid 参数名称为 ssid。

使用指南：本命令用于配置在重定向 url 中携带的 ssid 参数名称。

举例：配置重定向 url 中携带的 ssid 参数名称为 ssid。

Switch (config-cp-instance)#redirect attribute ssid name ssid

13.1.34 redirect attribute nas-ip enable

命令：redirect attribute nas-ip enable

no redirect attribute nas-ip enable

功能：使能重定向 url 中携带 nas-ip 参数功能。本命令的 no 形式为关闭重定向 url 中携带 nas-ip 参数的功能。

参数：无。

命令模式：captive portal instance 配置模式

缺省情况：缺省情况下重定向 url 中携带的 nas-ip 参数的功能是关闭的。

使用指南：本命令用户使能重定向 url 中携带 nas-ip 参数功能。使能此功能后，客户端进行重定向时，重定向的 url 中会携带客户端所关联的交换机的 IP 地址。

举例：使能重定向 url 中携带 nas-ip 参数功能。

Switch (config-cp-instance)#redirect attribute nas-ip enable

13.1.35 redirect attribute nas-ip name

命令：redirect attribute nas-ip name <word>

no redirect attribute nas-ip name

功能：配置在重定向 url 中携带的 nas-ip 参数的名称。本命令的 no 形式为恢复重定向 url 中携带的 nas-ip 参数的名称为默认值。

参数：<word>，为 nas-ip 参数名称。最多 32 个字节。

命令模式：captive portal instance 配置模式。

缺省情况：缺省情况下重定向 url 中携带的 nas-ip 参数的名称为 acname。

使用指南：本命令用于配置在重定向 url 中携带的 nas-ip 参数的名称。

举例：配置在重定向 url 中携带的 nas-ip 参数的名称为 nasip

Switch (config-cp-instance)#redirect attribute nas-ip name nasip

13.1.36 vlan-pool <1-255> <WORD>

命令：vlan-pool <1-255> <WORD>

no vlan-pool <1-255>

功能：在端口下指定 VLAN 开启认证时，首先配置 VLAN 池，在 VLAN 池里指定一个 VLAN 范围，或者某些 VLAN ID，将这个 VLAN 池绑定到端口上，可以指定某个 VLAN 开启认证。

No 操作为删除地址池。

参数：<1-255>：vlan-pool ID 号（索引）；

WORD：vlan id 列表。

缺省情况：无。

命令模式：全局配置模式。

使用指南：指定某个 VLAN 开启认证。配置 VLAN 池，检查 VLAN 池中的元素是否和其他 VLAN 池有重复。不允许更改已经绑定到端口的 VLAN 池里的元素。

举例：vlan 1-100 需要开启 portal 认证，配置地址池。

Switch(config)#vlan-pool 1 1-100

13.1.37 session-timeout

命令：session-timeout <0-86400>

no session-timeout

功能：定义 Captive Portal 配置的会话超时。该命令的 no 操作为关闭此功能。

参数：<0-86400>，会话超时时间，单位为秒，如果是 0 则表示超时功能未生效。

缺省情况：86400。

命令模式：Captive Portal Instance 配置模式。

使用指南：定义 Captive Portal 配置的会话超时。

举例：定义 Captive Portal 配置的会话超时时间为 100 秒。

Switch (config-cp-instance)# session-timeout 100

13.1.38 show captive-portal

命令：show captive-portal

功能：使用该命令显示 Captive Portal 的特征状态。

参数：无。

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示本交换机上的 captive portal 功能的相关状态参数。

举例：显示 Captive Portal 的开启和关闭状态。

captive portal 开启的情况：

Switch #show captive-portal

Administrative Mode..... Enable

Operational Status..... Enabled

CP IP Address..... 101.1.1.3

captive portal 关闭的情况：

switch#show captive-portal

Administrative Mode..... Disable

Operational Status..... Disabled

Disable Reason..... Administrator Disabled

CP IP Address..... 0.0.0.0

13.1.39 show captive-portal status

命令：show captive-portal status

功能：该命令显示系统中所有的 Captive Portal 例程的状态。

参数：无。

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示本交换机上的 captive portal 的配置和所支持属性参数。

举例：显示控制器上的 Captive Portal 的状态。

```
Switch #show captive-portal status
Peer Switch Statistics Reporting Interval..... 120
Authentication Timeout..... 300
Authentication Type..... External
Supported Captive Portals..... 10
Configured Captive Portals..... 9
Active Captive Portals..... 0
Local Supported Users..... 128
Configured Local Users..... 0
System Supported Users..... 1024
Authenticated Users..... 0
```

13.1.40 show captive-portal configuration

命令：show captive-portal configuration <cp-id>

功能：该命令显示了 Captive Portal 配置的状态。

参数：<cp-id>是 captive portal 的 ID 号，范围是 1-10。

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示 portal 的例程配置参数。

举例：显示 captive portal1 的配置情况。

```
Switch #show captive-portal configuration 1
CP ID..... 1
CP Name..... Default
Operational Status..... Enabled
Block Status..... Not Blocked
Configured Locales..... 1
Authenticated Users..... 0
Permit-all Status..... Disabled
```

13.1.41 show captive-portal configuration interface

命令：show captive-portal configuration <cp-id> interface <IFNAME or ethernet>

功能：该命令显示所有分配到 captive portal 配置的接口的信息。

参数：<cp-id>，cp 的 ID 号；

IFNAME ,Interface Name or number

Ethernet, Ethernet port

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示某个 portal 例程的接口状态。

举例：显示 Captive Portal 配置的接口信息。

Switch # show captive-portal configuration 1 interface e1/1

```
CP ID..... 1
CP Name..... Default
Interface..... 1
Interface Description..... Ethernet1/1
Operational Status..... Enabled
Block Status..... Not Blocked
Authenticated Users..... 0
```

13.1.42 show captive-portal configuration status

命令：show captive-portal configuration [<cp-id>] status

功能：该命令显示所有的或特定的 Captive Portal 的配置信息。

参数：<cp-id>，cp 的 ID 号，此处带有参数<cp-id>表示显示某个例程的内容，不带该参数显示当前所有配置的例程相关参数。

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示详细的 portal 例程配置参数。

举例：显示所有 Captive Portal 配置信息。

显示所有例程的状态：

Switch # show captive-portal configuration status

```
CP ID      CP Name      Mode    Protocol Verification
-----
```

```
1      Default      Enable  HTTP      RADIUS
2      Default      Enable  HTTP      RADIUS
```

13.1.43 show captive-portal client status

命令：show captive-portal client [<FF-FF-FF-FF-FF-FF> { ipv4 | ipv6 } <ip-addr>] status

功能：该命令显示了连接到 captive portal 的用户的详细连接信息或概述。

参数：<FF-FF-FF-FF-FF-FF>为用户的 MAC 地址

ipv4 用户地址为 ipv4 地址

ipv6 用户地址为 ipv6 地址

<ip-addr>用户地址，ipv4 地址是以点分十进制格式，ipv6 地址是 X:X::X:X 的格式

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示所有或某个 portal 用户的状态。

举例：显示连接到 captive portal 的用户 user1 的详细信息。

Switch # show captive-portal client status

MAC Address	IP Address	User Name	Protocol	Mode	Session Time
20-6a-8a-65-0d-17	66.1.1.2	user1	HTTP	RADIUS	0d:00:00:47

13.1.44 show captive-portal configuration client

命令：show captive-portal configuration [*<cp-id>*] client status

功能：该命令显示了某个接口下经过 portal 认证的客户端信息。

参数：*<cp-id>*，Captive Portal 的 ID 号。

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示某个 portal 例程上的用户参数。

举例：显示经过认证的客户端的所有 captive portal 配置信息。

Switch #show captive-portal configuration 1 client status

CP ID..... 1

CP Name..... Default

Client MAC Address	Client IP Address	Interface	Interface Description
00-24-8c-00-99-27	10.1.1.51	1922	Port-Channel2

13.1.45 show captive-portal ext-portal-server status

命令：show captive-portal ext-portal-server status

功能：使用该命令查看配置的外置 portal 服务器的信息。

参数：无。

缺省情况：无。

命令模式：特权模式。

使用指南：查看配置的外置 portal 服务器的信息。

举例：查看配置的外置 portal 服务器的信息。

Switch #show captive-portal ext-portal-server status

Server Name	Server IP Address	port	SocketNo
x1	100.1.1.2	7749	0
x2	100.1.1.1	7749	0

13.1.46 show captive-portal interface configuration status

命令：show captive-portal interface configuration [*<cp-id>*] status

功能：该命令显示为所有的 captive portal 配置或特定的配置的接口信息。

参数：*<cp-id>*，captive portal 的ID号。

缺省情况：无。

命令模式：特权模式

使用指南：该命令显示所有或某个portal例程与接口的绑定关系。

举例：显示为所有的 captive portal 配置的接口信息。

Switch #show captive-portal interface configuration status

CP ID	CP Name	Interface	Interface Description	Type
1	Default	1	Ethernet1/1	Physical

13.2 Free-resource 命令

13.2.1 free-resource（全局）

命令：free-resource destination { ipv4 | ipv6 } <ip-addr><netmask> }

no free-resource destination { ipv4 | ipv6 } <ip-addr><netmask> }

功能：该命令配置 free-resource 规则，符合规则中源 IP 地址段的客户端访问规则中目的 IP 地址段的资源，交换机不进行重定向，客户端不需要通过 Portal 认证可以直接访问。

参数：

ipv4 配置的 free resource 地址是 ipv4 地址

ipv6 配置的 free resource 地址是 ipv6 地址

<ip-addr> free-resource 规则中被访问/访问者的 IP 地址段

<netmask> free-resource 规则中被访问/访问者的 IP 地址段

缺省情况：无。

命令模式：全局配置模式。

使用指南：配置可以免费访问资源的客户端地址段（访问者）和免费提供该资源的地址段（被访问者）。

举例：配置 free-resource 规则。

Switch (config)# free-resource destination ipv4 1.1.1.1/24

13.3 认证白名单

13.3.1 free-mac

命令：free-mac < MACADD>< MACMASK>

no free-mac < MACADD>< MACMASK>

功能：添加免认证 MAC，no 命令用来删除配置的免认证 MAC。

参数：< MACADD> mac 地址；

< MACMASK>mac 掩码。

缺省情况：无。

命令模式：全局配置模式。

使用指南：对于指定 MAC 的用户免认证的含义是直接放行，可以不经任何认证。

举例：配置免认证 MAC 00-01-11-11-11-11。

Switch(Config)#free-mac 00-01-11-11-11-11

13.4 认证成功页面自动推送命令（暂不支持）

13.4.1 redirect attribute url-after-login enable

命令：redirect attribute url-after-login enable

no redirect attribute url-after-login enable

功能：使能重定向 url 中携带认证成功后推送 url 地址的功能。本命令的 no 形式为关闭重定向 url 中携带认证成功后推送 url 地址的功能。

参数：无。

命令模式：captive portal instance 配置模式

缺省情况：缺省情况下重定向 url 中携带认证成功后推送 url 地址的功能是关闭的。

使用指南：本命令用于使能重定向 url 中携带认证成功后推送 url 地址的功能。使能改功能后，交换机推出的重定向 url 中会携带认证成功后需要推送的 url 地址，同时当 redirect attribute url-after-login value 配置的<url-value>为空时，携带的 url 地址为用户认证前访问的页面地址，若不为空，则携带的 url 地址为<url-value>所配置的地址。

举例：使能重定向 url 中携带认证成功后推送 url 地址的功能。

Switch (config-cp-instance)#redirect attribute url-after-login enable

13.4.2 redirect attribute url-after-login name

命令：redirect attribute url-after-login name <name>

no redirect attribute url-after-login name

功能：配置在重定向 url 中携带认证成功后推送 url 地址的属性值名称。本命令的 no 形式为恢复重定向 url 中携带认证成功后推送 url 地址的属性值名称为默认值。

参数：<name>，为配置的属性值名称。最多 32 个字符。

命令模式：captive portal instance 配置模式。

缺省情况：缺省情况下重定向 url 中携带认证通过后推送 url 地址的属性值名称为 srcurl。

使用指南：本命令用于配置在重定向 url 中携带认证成功后推送 url 地址的属性值名称。

举例：配置在重定向 url 中携带认证成功后推送 url 地址的属性值名称为 redirect

Switch (config-cp-instance)#redirect attribute url-after-login name redirect

13.4.3 redirect attribute url-after-login encode

命令：redirect attribute url-after-login encode {plain-text|base64}

功能：配置对重定向 url 中携带的认证成功后推送 url 地址的编码方式。

参数：plain-text，为明文方式；

base64，为 base64 编码方式。

命令模式：captive portal instance 配置模式。

缺省情况：缺省情况下重定向 url 中携带的认证成功后推送 url 地址的编码方式为 plain-text

明文方式。

使用指南：本命令用于配置对重定向 url 中携带的认证成功后推送 url 地址的编码方式。可以根据 portal server 所支持的编码方式来配置。

举例：配置对重定向 url 中携带的认证成功后推送 url 地址的编码方式为 base64 编码方式。
Switch (config-cp-instance)#redirect attribute url-after-login encode base64

13.4.4 redirect attribute url-after-login value

命令：redirect attribute url-after-login value <url-value>
no redirect attribute url-after-login value

功能：配置用户认证成功后弹出的指定页面的 url 地址。本命令的 no 形式为删除用户认证成功后弹出的指定页面的 url 地址。

参数：<url-value>，为配置的指定页面的 url 地址。最多 512 个字符。

命令模式：captive portal instance 配置模式。

缺省情况：无。

使用指南：本命令用户配置用户认证成功后弹出的指定页面的 url 地址。如果开启重定向 url 中携带认证成功后推送的 URL 地址的功能，这样在重定向 url 中会携带值为<url-value>的指定页面的 URL 地址。

举例：配置用户认证成功后弹出的指定页面的 url 地址为 http://www.test.com。

Switch (config-cp-instance)#redirect attribute url-after-login value http://www.test.com

13.5 Portal 无感知命令

13.5.1 fast-mac-auth

命令：fast-mac-auth
no fast-mac-auth

功能：该命令配置开启 mac 快速认证功能。no 操作为关闭 mac 快速认证。

参数说明：无。

命令模式：Captive Portal Instance 模式。

默认配置：默认关闭。

使用指南：使能该功能后，如果 mac 认证成功，则不需要进行 portal 认证。

举例：开启 mac 快速认证功能。

Switch (config-cp-instance)#fast-mac-auth

13.6 Portal 逃生命令

13.6.1 portal-server-detect server-name <name>

命令：portal-server-detect server-name <name> [interval <interval>] [retry

<retries>][action {log | permit-all | trap }]

no portal-server-detect server-name <name>

功能：开启 Portal server 的逃生功能，并配置相关的检测参数和服务器状态变化时的操作。

参数：<name>为 Portal 服务器名称，为 1~32 个字符的字符串，区分大小写。该 Portal 服务器必须已经存在。<interval>：进行探测尝试的时间间隔，取值范围为 20~600，单位为秒，缺省值为 20。<retries>：连续探测失败的最大次数，取值范围为 1~5，缺省值为 3。若连续探测失败数目达到此值，则认为服务器不可达。{ log | permit-all | trap }：Portal 服务器可达状态发生变化时，可触发执行的操作。包括以下三种，且同时可选择多种。

- ☞ **log：**Portal 服务器状态发生改变时，发送日志信息。日志信息中记录了 Portal 服务器名称以及该服务器状态改变前后的状态信息。
- ☞ **trap：**Portal 服务器状态发生改变时，向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal 服务器名称以及该服务器状态改变前后的状态信息。
- ☞ **permit-all：**也称为 Portal 逃生，表示在 Portal 服务器不可达（down）时，暂时取消 Portal 认证，允许所有 Portal 用户访问网络资源。之后，若服务器状态变为可达（up）时，恢复其 Portal 认证功能。

缺省情况：逃生功能关闭。interval 缺省为 20，retries 缺省为 3，action 缺省为 permit-all。

命令模式：Captive Portal 全局配置模式。

使用指南：为了保证 Portal server 发生故障时，可以用该命令打开 Portal 逃生功能。打开 Portal 逃生功能后，如果交换机和 Portal server 连接正常，对于用户 Portal 认证没有任何影响；只有当交换机和 Portal server 连接中断时，才会允许用户不通过认证就可以访问网络。运营商也可以打开逃生功能，但是触发的操作只选择 log 或 trap。

举例：打开名称为 test 的 Portal server 的逃生功能,探测周期为 30 秒，最大失败次数为 2，服务器状态变化时触发的操作为发送日志和允许用户接入网络。

```
Switch (config-cp)# portal-server-detect server-name test interval 600 retry 2 action log permit-all trap
```

13.6.2 portal-server-detect client-deauth

命令：portal-server-detect client-deauth

no portal-server-detect client-deauth

功能：开启此命令，则服务器状态从 down 转变为 up 后，所有用户强制下线。no 操作为关闭此命令，则配置 Portal 服务器探测状态从 down 转变为 up 后，不强制已经在线的用户下线。

参数：无。

缺省情况：默认开启。

命令模式：captive portal 模式。

使用指南：该命令默认开启，即默认配置为所有用户在服务器状态该变时强制下线。隐藏命令，show run 不能看到。

```
Switch (config-cp)# portal-server-detect client-deauth
```

13.6.3 show captive-portal ext-portal-server server-name <name> status

命令：show captive-portal ext-portal-server server-name <name> status

功能：显示 Portal server 的状态，包括服务器地址、是否启动 Portal 逃生等信息。

参数：<name>为 Portal 服务器名称，为 1~32 个字符的字符串，区分大小写。

缺省情况：无。

命令模式：特权模式。

使用指南：检查服务器的状态是进行故障检查的重要手段，当 Portal 逃生功能没有生效时，也许是配置错误，通过改命令能帮助管理员排错。如果不带<name>参数则显示所有的服务器的概要状态，如果带<name>参数则显示该服务器的详细状态。

举例：显示所有的外置 Portal server 的状态。

显示名称为 Portaltest 的服务器的详细状态

```
Switch (config-cp)#show captive-portal ext-portal-server server-name Portaltest status
```

```
Server Name..... portaltest
Server IP..... 101.1.1.6
Server Port..... 7749
Server Key.....
Detect Mode..... Enable
Detect Interval..... 20
Detect Retries..... 3
Detect Trap Mode..... Disable
Detect Log Mode..... Disable
Detect Permit-all Mode..... Enable
Detect Operational Mode..... Enable
Detect Operational Status..... Down
Detect Operational Fails..... 1
Detect Operational Time..... 0d:00:00:11
```