

目 录

第 1 章 ACL配置	1-1
1.1 ACL介绍	1-1
1.1.1 Access-list	1-1
1.1.2 Access-group	1-1
1.1.3 Access-list动作及全局默认动作.....	1-1
1.2 ACL配置	1-2
1.3 ACL举例	1-19
1.4 ACL排错帮助	1-23
第 2 章 802.1x配置	2-1
2.1 802.1x介绍	2-1
2.1.1 802.1x认证体系结构	2-1
2.1.2 802.1x工作机制.....	2-2
2.1.3 EAPOL消息的封装.....	2-3
2.1.4 EAP属性的封装.....	2-4
2.1.5 基于 802.1x的Web认证代理功能	2-5
2.1.6 802.1x认证方式.....	2-6
2.1.7 802.1x的扩展和优化	2-10
2.1.8 VLAN分配特性	2-11
2.2 802.1x配置	2-12
2.3 802.1x应用举例	2-15
2.3.1 Guest Vlan应用举例.....	2-15
2.3.2 802.1x与IPv4 Radius应用举例	2-17
2.3.3 802.1x与IPv6 Radius应用举例	2-18
2.3.4 基于 802.1x的Web认证代理应用举例.....	2-19
2.4 802.1x排错帮助	2-21
第 3 章 端口、VLAN中MAC、IP 数量限制功能配置	3-1
3.1 端口、VLAN中MAC、IP 数量限制功能简介	3-1
3.2 端口、VLAN中MAC、IP数量限制功能配置任务序列	3-2
3.3 端口、VLAN中MAC、IP数量限制功能典型案例	3-4
3.4 端口、VLAN中MAC、IP数量限制功能排错帮助	3-4

第 4 章 AM功能操作配置	4-1
4.1 AM功能简介	4-1
4.2 AM功能配置任务序列	4-1
4.3 AM功能典型案例	4-3
4.4 AM功能排错帮助	4-3
第 5 章 安全特性配置	5-1
5.1 安全特性介绍	5-1
5.2 安全特性配置	5-1
5.2.1 防IP Spoofing功能配置任务序列	5-1
5.2.2 防TCP非法标志攻击功能配置任务序列	5-1
5.2.3 防端口欺骗功能配置任务序列	5-1
5.2.4 防TCP碎片攻击功能配置任务序列	5-2
5.2.5 防ICMP碎片攻击功能配置任务序列	5-2
5.3 安全特性举例	5-3
第 6 章 TACACS+配置	6-1
6.1 TACACS+简介	6-1
6.2 TACACS+配置	6-1
6.3 TACACS+典型案例	6-2
6.4 TACACS+排错帮助	6-2
第 7 章 RADIUS配置	7-1
7.1 RADIUS简介	7-1
7.1.1 AAA与RADIUS简介	7-1
7.1.2 RADIUS协议的报文结构	7-1
7.2 RADIUS配置	7-3
7.3 RADIUS典型案例	7-5
7.3.1 IPv4 Radius应用举例	7-5
7.3.2 IPv6 Radius应用举例	7-5
7.4 RADIUS排错帮助	7-6
第 8 章 SSL配置	8-1
8.1 SSL简介	8-1

8.1.1 SSL基本原理.....	8-1
8.2 SSL配置任务序列	8-2
8.3 SSL典型案例	8-3
8.4 SSL排错帮助	8-4
第 9 章 IPv6 安全RA配置.....	9-1
9.1 IPv6 安全RA简介	9-1
9.2 IPv6 安全RA配置任务序列	9-1
9.3 IPv6 安全RA典型案例.....	9-2
9.4 IPv6 安全RA排错帮助.....	9-2
第 10 章 VLAN-ACL配置	10-1
10.1 VLAN-ACL功能简介	10-1
10.2 VLAN-ACL功能配置任务序列.....	10-1
10.3 VLAN-ACL功能配置案例.....	10-3
10.4 VLAN-ACL排错帮助	10-4
第 11 章 MAB配置	11-1
11.1 MAB介绍	11-1
11.2 MAB基本配置	11-1
11.3 MAB举例	11-3
11.4 MAB排错帮助	11-6

第1章 ACL配置

1.1 ACL介绍

ACL (Access Control Lists)是交换机实现的一种数据包过滤机制，通过允许或拒绝特定的数据包进入网络，交换机可以对网络访问进行控制，有效保证网络的安全运行。用户可以基于报文中的特定信息制定一组规则（rule），每条规则都描述了对匹配一定信息的数据包所采取的动作：允许通过（permit）或拒绝通过（deny）。用户可以把这些规则应用到特定交换机端口的入口，这样特定端口上特定方向的数据流就必须依照指定的 ACL 规则进入交换机。

1.1.1 Access-list

Access-list是一个有序的语句集，每一条语句对应一条特定的规则(rule)。每条rule包括了过滤信息及匹配此rule时应采取的动作。Rule包含的信息可以包括源MAC、目的MAC、源IP、目的IP、IP协议号、TCP端口、UDP端口等条件的有效组合。根据不同的标准，access-list可以有如下分类：

- ☞ 根据过滤信息：ip access-list, ipv6 access-list（三层以上信息），mac access-list（二层信息），mac-ip access-list（二层以上信息）。
- ☞ 根据配置的复杂程度：标准(standard)和扩展(extended)，扩展方式可以指定更加细致过滤信息。
- ☞ 根据命名方式：数字(numbered)和命名(named)。

对一条ACL的说明应当从这三个方面加以描述。

1.1.2 Access-group

当用户按照实际需要制定了一组access-list之后，就可以把他们分别应用到不同端口的入口方向上。access-group就是对特定的一条access-list与特定端口的绑定关系的描述。当您建立了一条access-group之后，流经此端口此方向的所有数据包都会试图匹配指定的access-list规则，以决定交换动作是允许(permit)或拒绝(deny)。另外还可以在端口加上对ACL规则统计计数器，以便统计符合ACL规则数据包的数量。

1.1.3 Access-list动作及全局默认动作

Access-list动作及默认动作分为两种：允许通过(permit)或拒绝通过(deny)。具体有如下：

- ☞ 在一个access-list内，可以有多条规则(rule)。对数据包的过滤从第一条规则(rule)开始，直到匹配到一条规则(rule)，其后的规则(rule)不再进行匹配。全局默

认动作只对端口入口方向的数据流量有效。

- ✎ 只有在包过滤功能打开且端口上没有绑定任何的ACL或不匹配任何绑定的ACL时才会匹配入口的全局的默认动作。

1.2 ACL配置

ACL配置任务序列如下：

1. 配置 access-list

- (1) 配置数字标准 IP 访问列表
- (2) 配置数字扩展 IP 访问列表
- (3) 配置命名标准 IP 访问列表
 - a) 创建一个命名标准 IP 访问列表
 - b) 指定多条 permit 或 deny 规则表项
 - c) 退出访问表配置模式
- (4) 配置命名扩展 IP 访问列表
 - a) 创建一个命名扩展 IP 访问列表
 - b) 指定多条 permit 或 deny 规则表项
 - c) 退出访问表配置模式
- (5) 配置数字标准 MAC 访问列表
- (6) 配置数字扩展 MAC 访问列表
- (7) 配置命名扩展 MAC 访问列表
 - a) 创建一个命名扩展 MAC 访问列表
 - b) 指定多条 permit 或 deny 规则表项
 - c) 退出 MAC 访问表配置模式
- (8) 配置数字扩展 MAC-IP 访问列表
- (9) 配置命名扩展 MAC-IP 访问列表
 - a) 创建一个命名扩展 MAC-IP 访问列表
 - b) 指定多条 permit 或 deny 规则表项
 - c) 退出 MAC-IP 访问表配置模式
- (10) 配置数字标准 IPv6 访问列表
- (11) 配置数字扩展 IPv6 访问列表
- (12) 配置命名标准 IPv6 访问列表
 - a) 创建一个命名标准 IPv6 访问列表
 - b) 指定多条 permit 或 deny 规则表项
 - c) 退出 IPv6 访问表配置模式
- (13) 配置命名扩展 IPv6 访问列表
 - a) 创建一个命名扩展 IPv6 访问列表
 - b) 指定多条 permit 或 deny 规则表项
 - c) 退出 IPv6 访问表配置模式

2. 配置包过滤功能
 - (1) 全局打开包过滤功能
 - (2) 全局配置 ACL deny 优先功能模块（可选）
3. 配置时间范围功能
 - (1) 创建时间范围名称
 - (2) 配置周期性时段
 - (3) 配置绝对性时段
4. 将 access-list 绑定到特定端口的特定方向
5. 清空指定接口的包过滤统计信息

1. 配置 access-list

(1) 配置数字标准 IP 访问列表

命令	解释
全局配置模式	
access-list <num> {deny permit} {<slpAddr> <sMask> any-source {host-source <slpAddr>}} no access-list <num>	创建一条数字标准 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项；本命令的 no 操作为删除一条数字标准 IP 访问列表。

(2) 配置数字扩展 IP 访问列表

命令	解释
全局配置模式	
access-list <num> {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>]	创建一条 ICMP 数字扩展 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。
access-list <num> {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>]	创建一条 IGMP 数字扩展 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。

<pre>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>]</pre>	创建一条 TCP 数字扩展 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。
<pre>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>]</pre>	创建一条 UDP 数字扩展 IP 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。
<pre>access-list <num> {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>]</pre>	创建一条匹配其他特定 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，则增加一条规则（rule）表项。
no access-list <num>	删除一条数字扩展 IP 访问列表。

(3) 配置命名标准 IP 访问列表

a. 创建一个命名标准 IP 访问列表

命令	解释
全局配置模式	
<pre>ip access-list standard <name> no ip access-list standard <name></pre>	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。

b. 指定多条 permit 或 deny 规则

命令	解释
命名标准 IP 访问列表配置模式	
<pre>[no] {deny permit} {{<slpAddr> <sMask >} any-source {host-source <slpAddr>}}</pre>	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）。

c. 退出命名标准 IP 访问列表配置模式

命令	解释
命名标准 IP 访问列表配置模式	
exit	退出命名标准 IP 访问列表配置模式。

(4) 配置命名扩展 IP 访问列表

a. 创建一个命名扩展 IP 访问列表

命令	解释
全局配置模式	
ip access-list extended <name> no ip access-list extended <name>	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。

b. 指定多条 permit 或 deny 规则

命令	解释
命名扩展 IP 访问列表配置模式	
[no] {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>]	创建一条 icmp 命名扩展 IP 访问规则 (rule)；本命令的 no 操作为删除此命名扩展 IP 访问规则 (rule)。
[no] {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>]	创建一条 igmp 命名扩展 IP 访问规则 (rule)；本命令的 no 操作为删除此命名扩展 IP 访问规则 (rule)。
[no] {deny permit} tcp {{<slpAddr> <sMask>} any-source {host-source <slpAddr>}} [s-port {<sPort> range <sPortMin> <sPortMax>}] {{<dlpAddr> <dMask>} any-destination {host-destination <dlpAddr>}} [d-port {<dPort> range <dPortMin> <dPortMax>}] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range<time-range-name>]	创建一条 tcp 命名扩展 IP 访问规则 (rule)；本命令的 no 操作为删除此命名扩展 IP 访问规则 (rule)。

<pre>[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>]</pre>	创建一条 udp 命名扩展 IP 访问规则 (rule)；本命令的 no 操作为删除此命名扩展 IP 访问规则(rule)。
<pre>[no] {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>]</pre>	创建一条匹配其他特定 IP 协议或所有 IP 协议的数字扩展 IP 访问规则；如果此编号数字扩展访问列表不存在则创建此访问列表。

c. 退出命名扩展 IP 访问列表配置模式

命令	解释
命名扩展 IP 访问列表配置模式	
exit	退出命名扩展 IP 访问列表配置模式。

(5) 配置数字标准 MAC 访问列表

命令	解释
全局配置模式	
<pre>access-list <num> {deny permit} {any-source-mac {host-source-mac <host_smac>} {<smac> <smac-mask>}} no access-list <num></pre>	创建一条数字标准 mac 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 操作为删除一条数字标准 mac 访问列表。

(6) 配置数字扩展 MAC 访问列表

命令	解释
全局配置模式	

<pre>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></pre>	创建一条数字扩展 mac 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 操作为删除一条数字扩展 mac 访问列表。
--	--

(7) 配置命名扩展 MAC 访问列表

a. 创建一个命名扩展 MAC 访问列表

命令	解释
全局配置模式	
mac-access-list extended <name> no mac-access-list extended <name>	创建一条命名扩展 MAC 访问列表；本命令的 no 操作为删除此命名扩展 MAC 访问列表。

b. 指定多条 permit 或 deny 规则表项

命令	解释
命名扩展 MAC 访问列表配置模式	

<pre>[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>]]</pre> <pre>[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>]]</pre> <pre>[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>]]]</pre>	创建一条匹配普通 MAC 帧的命名扩展 MAC 访问规则(rule); no 操作为删除此命名扩展 MAC 访问规则 (rule)
<pre>[no]{deny permit}{any-source-mac {host-source-mac<host _smac>}}{<smac><smac-mask>}}{any-destination-mac {ho st-destination-mac<host_dmac>}}{<dmac><dmac-mask>}} [untagged-eth2 [ethertype <protocol> [protocol-mask]]]</pre>	创建一条匹配 untagged 以太网 2 帧类型的命名扩展 MAC 访问规则(rule); no 操作为删除此命名扩展 MAC 访问规则 (rule)
<pre>[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]</pre>	创建一条匹配 untagged 802.3 帧类型的命名扩展 MAC 访问规则(rule); no 操作为删除此命名扩展 MAC 访问规则 (rule)
<pre>[no]{deny permit}{any-source-mac {host-source-mac<host _smac>}}{<smac><smac-mask>}}{any-destination-mac {ho st-destination-mac<host_dmac>}}{<dmac><dmac-mask>}}[tagged-eth2 [cos <cos-val> [<cos-bitmask>]] [vlanId <vid-value> [<vid-mask>]] [ethertype<protocol> [<protocol-mask>]]]</pre>	创建一条匹配 tagged 以太网 2 帧类型的命名扩展 MAC 访问规则 (rule); no 操作为删除此命名扩展 MAC 访问规则 (rule)

<code>[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>]]]</code>	创建一条匹配 tagged 802.3 帧类型的命名扩展 MAC 访问规则 (rule); no 操作为删除此命名扩展 MAC 访问规则 (rule)
--	---

c. 退出 MAC 访问表配置模式

命令	解释
命名扩展 MAC 访问列表配置模式	
exit	退出命名扩展 MAC 访问列表配置模式

(8) 配置数字扩展 MAC-IP 访问列表

命令	解释
全局配置模式	
<code>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>]</code>	创建一条 MAC-ICMP 数字扩展 mac-ip 访问列表, 如果已有此访问列表, 则增加一条规则 (rule) 表项。
<code>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>]</code>	创建一条 MAC-IGMP 数字扩展 mac-ip 访问列表, 如果已有此访问列表, 则增加一条规则 (rule) 表项。

<pre>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>]</pre>	创建一条 MAC-TCP 数字扩展 mac-ip 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。
<pre>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>]</pre>	创建一条 MAC-UDP 数字扩展 mac-ip 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。
<pre>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>]</pre>	创建一条匹配其他特定 MAC-IP 协议或所有 MAC-IP 协议的数字扩展 mac-ip 访问列表，如果已有此访问列表，则增加一条规则（rule）表项。
<pre>no access-list <num></pre>	删除一条数字扩展 MAC-IP 访问列表。

(9) 配置命名扩展 MAC-IP 访问列表

a. 创建一个命名扩展 MAC-IP 访问列表

命令	解释
全局配置模式	
mac-ip-access-list extended <name> no mac-ip-access-list extended <name>	创建一条命名扩展 MAC-IP 访问列表; 本命令的 no 操作为删除此命名扩展 MAC-IP 访问列表。

b. 指定多条 permit 或 deny 规则表项

命令	解释
命名扩展 MAC-IP 访问列表配置模式	
[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>]	创建一条 mac-icmp 命名扩展 MAC 访问规则 (rule); no 操作为删除此命名扩展 MAC-IP 访问规则 (rule)。
[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>]	创建一条 mac-igmp 命名扩展 MAC-IP 访问规则 (rule); no 操作为删除此命名扩展 MAC-IP 访问规则 (rule)。

<pre>[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>]</pre>	创建一条 mac-tcp 命名扩展 MAC-IP 访问规则 (rule); no 操作为删除此命名扩展 MAC-IP 访问规则 (rule)。
<pre>[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>]</pre>	创建一条 mac-udp 命名扩展 MAC-IP 访问规则 (rule); no 操作为删除此命名扩展 MAC-IP 访问规则 (rule)。
<pre>[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>]</pre>	创建一条 mac-ip 其他协议类型的命名扩展 MAC-IP 访问规则 (rule); no 操作为删除此命名扩展 MAC-IP 访问规则 (rule)。

c. 退出 MAC-IP 访问表配置模式

命令	解释
命名扩展 MAC-IP 访问列表配置模式	

exit	退出命名扩展 MAC-IP 访问列表配置模式
-------------	------------------------

(10) 配置数字标准 IPv6 访问列表

命令	解释
全局配置模式	
ipv6 access-list <num> {deny permit} [{<sIPv6Addr> <sPrefixlen>} any-source {host-source <sIPv6Addr>}] no ipv6 access-list <num>	创建一条数字标准 IPv6 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 操作为删除一条数字标准 IPv6 访问列表。

(11) 配置数字扩展 IPv6 访问列表

命令	解释
全局配置模式	

<pre> 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> </pre>	创建一条数字扩展 IPV6 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 操作为删除一条数字标准 IP 访问列表。
---	--

(12) 配置命名标准 IPv6 访问列表

a) 创建一个命名标准 IPv6 访问列表

命令	解释
全局配置模式	

ipv6 access-list standard <name> no ipv6 access-list standard <name>	创建一条命名标准 IPv6 访问列表；本命令的 no 操作为删除此命名标准 IPv6 访问列表。
---	--

b) 指定多条 permit 或 deny 规则

命令	解释
命名标准 IPv6 访问列表配置模式	
[no] {deny permit} {{<sIPv6Prefix/sPrefixlen>} any-source {host-source <sIPv6Addr>}}	创建一条命名标准 IPv6 访问规则（rule）；本命令的 no 操作为删除此命名标准 IPv6 访问规则（rule）。

c) 退出命名标准 IPv6 访问列表配置模式

命令	解释
命名标准 IPv6 访问列表配置模式	
exit	退出命名标准 IPv6 访问列表配置模式。

(13) 配置命名扩展 IPv6 访问列表

a) 创建一个命名扩展 IPv6 访问列表

命令	解释
全局配置模式	
ipv6 access-list extended <name> no ipv6 access-list extended <name>	创建一条命名扩展 IPv6 访问列表；本命令的 no 操作为删除此命名扩展 IPv6 访问列表。

b) 指定多条 permit 或 deny 规则

命令	解释
命名扩展 IP 访问列表配置模式	
[no] {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>]	创建一条 icmp 命名扩展 IPv6 访问规则（rule）；本命令的 no 操作为删除此命名扩展 IPv6 访问规则（rule）。

[no] {deny permit} tcp {<IPv6Prefix/sPrefixlen> any-source {host-source <IPv6Addr>}} [s-port {<Port> range <PortMin> <PortMax>}] {<IPv6Prefix/dPrefixlen> any-destination {host-destination <IPv6Addr>}} [d-port {<Port> range <PortMin> <PortMax>}] [syn ack urg rst fin psh] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	创建一条 tcp 命名扩展 IPv6 访问规则 (rule); 本命令的 no 操作为删除此命名扩展 IPv6 访问规则 (rule)。
[no] {deny permit} udp {<IPv6Prefix/sPrefixlen> any-source {host-source <IPv6Addr>}} [s-port {<Port> range <PortMin> <PortMax>}] {<IPv6Prefix/dPrefixlen> any-destination {host-destination <IPv6Addr>}} [d-port {<Port> range <PortMin> <PortMax>}] [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	创建一条 udp 命名扩展 IPv6 访问规则 (rule); 本命令的 no 操作为删除此命名扩展 IPv6 访问规则 (rule)。
[no] {deny permit} <proto> {<IPv6Prefix/sPrefixlen> any-source {host-source <IPv6Addr>}} {<IPv6Prefix/dPrefixlen> any-destination {host-destination <IPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	创建一条匹配其他特定 IPv6 协议的数字扩展 IPv6 访问规则; 如果此编号数字扩展访问列表不存在则创建此访问列表。
[no] {deny permit} {<IPv6Prefix/sPrefixlen> any-source {host-source <IPv6Addr>}} {<IPv6Prefix/dPrefixlen> any-destination {host-destination <IPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]	创建一条命名扩展 IPv6 访问规则 (rule); 本命令的 no 操作为删除此命名扩展 IPv6 访问规则 (rule)。

c) 退出命名扩展 IPv6 访问列表配置模式

命令	解释
命名扩展 IPv6 访问列表配置模式	
exit	退出命名扩展 IPv6 访问列表配置模式。

2. 配置包过滤功能

(1) 全局打开包过滤功能

命令	解释
全局配置模式	
firewall enable	全局打开包过滤功能。

firewall disable	全局关闭包过滤功能。
-------------------------	------------

(2) 配置 ACL deny 优先功能

命令	解释
全局配置模式	
[no] access-list deny-preemption	开启 acl deny 优先功能, 本命令的 no 操作为关闭 acl deny 优先功能。

3. 配置时间范围功能

(1) 创建时间范围名称

命令	解释
全局配置模式	
time-range <time_range_name>	创建一个名为 time_range_name 的时间范围名
no time-range <time_range_name>	停止名为 time_range_name 的时间范围功能

(2) 配置周期性时段

命令	解释
时间范围模式	
absolute-periodic {Monday Tuesday Wednesday Thursday Friday Saturday Sunday} <start_time> to {Monday Tuesday Wednesday Thursday Friday Saturday Sunday} <end_time>	配置一周内的各种不同要求的时间范围, 每周都循环这个时间
periodic {{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday} daily weekdays weekend} <start_time> to <end_time>	

<pre>[no] absolute-periodic {Monday Tuesday Wednesday Thursday Friday Saturday Sunday} <start_time> to {Monday Tuesday Wednesday Thursday Friday Saturday Sunday} <end_time></pre>	停止一周内的时间范围配置
<pre>[no] periodic {{Monday+Tuesday+Wednesday+ Thursday+Friday+Saturday+ Sunday} daily weekdays weekend} <start_time> to <end_time></pre>	

(3) 配置绝对性时段

命令	解释
全局配置模式	
<pre>absolute start <start_time> <start_data> [end <end_time> <end_data>]</pre>	创建一个绝对时间范围
<pre>[no] absolute start <start_time> <start_data> [end <end_time> <end_data>]</pre>	停止一个绝对时间范围功能

4. 将 access-list 绑定到特定端口的特定方向

命令	解释
物理接口配置模式/Vlan 接口模式	
<pre>{ip ipv6 mac mac-ip} access-group <acl-name> {in out} [traffic-statistic] no {ip ipv6 mac mac-ip} access-group <acl-name> {in out}</pre>	物理接口模式：在端口的入口或出口方向上应用一条 access-list；no 操作为删除绑定在端口上的 access-list。

5. 清空指定接口的包过滤统计信息

命令	解释
特权用户模式	

<pre>clear access-group (in out) statistic interface { <interface-name> ethernet <interface-name> }</pre>	在指定端口清除出口或入口方向包过滤统计信息。
--	------------------------

1.3 ACL 举例

案例 1:

用户有如下配置需求：交换机的端口 10 连接 10.0.0.0/24 网段，管理员不希望用户使用 ftp。

配置更改：

- a) 创建相应的 ACL
- b) 配置包过滤功能
- c) 绑定 ACL 到端口

配置步骤如下：

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
```

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

```
Switch(config)#firewall default permit
```

```
Switch(config)#interface ethernet1/0/10
```

```
Switch(Config-If-Ethernet1/0/10)#ip access-group 110 in
```

```
Switch(Config-If-Ethernet1/0/10)#exit
```

```
Switch(config)#exit
```

配置结果：

```
Switch#show firewall
```

```
Firewall Status: Enable.
```

```
Firewall Default Rule: Permit.
```

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

```
access-list 110(used 1 time(s)) 1 rule(s)
```

```
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
```

```
Switch#show access-group interface ethernet 1/0/10
```

```
interface name:Ethernet1/0/10
```

```
IP Ingress access-list used is 110, traffic-statistics Disable.
```

案例 2:

用户有如下配置需求：交换机的端口 10 不允许转发源 MAC 地址是 00-12-11-23-XX-XX

的 802.3 的数据报文。

配置更改：

- 1、创建相应的 MAC ACL
- 2、配置包过滤功能
- 3、绑定 ACL 到端口

配置步骤如下：

```
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac untagged-802-3
Switch(config)# access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any
tagged-802
Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#mac access-group 1100 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit
```

配置结果：

```
Switch#show firewall
Firewall Status: Enable.
Firewall Default Rule: Permit.
Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
untagged-802-3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
MAC Ingress access-list used is 1100,traffic-statistics Disable.
```

案例 3：

用户有如下配置需求：交换机的端口 10 连接的网段的 MAC 地址是 00-12-11-23-XX-XX，并且 IP 为 10.0.0.0/24 网段，管理员不希望用户使用 ftp，也不允许外网 ping 此网段的任何一台主机。

配置更改：

- ◇ 创建相应的 ACL
- ◇ 配置包过滤功能

☞ 绑定 ACL 到端口

配置步骤如下：

```
Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff  
any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
```

```
Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00  
00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255
```

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

```
Switch(config)#firewall default permit
```

```
Switch(config)#interface ethernet 1/0/10
```

```
Switch(Config-If-Ethernet1/0/10)#mac-ip access-group 3110 in
```

```
Switch(Config-Ethernet1/0/10)#exit
```

```
Switch(config)#exit
```

配置结果：

```
Switch#show firewall
```

```
Firewall Status: Enable.
```

```
Firewall Default Rule: Permit.
```

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

```
access-list 3110(used 1 time(s))
```

```
access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff  
any-destination-mac
```

```
tcp 10.0.0.0 0.0.0.255 any-destination d-port 21
```

```
access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp  
any-source 10.0.0.0 0.0.0.255
```

```
Switch#show access-group interface ethernet 1/0/10
```

```
interface name: Ethernet1/0/10
```

```
MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.
```

案例 4：

用户有如下配置需求：交换机的 600 端口连接的网段是 IPV6，并且 IPV6 的地址为 2003:

1: 1: 1:: 0/64 网段，管理员不希望除了 2003: 1: 1: 66:: 0/80 网段用户访问外网。

配置更改：

1、创建相应的 ACL

2、配置包过滤功能

3、绑定 ACL 到端口

配置步骤如下：

```
Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-destination
```

```
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-destination
```

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

```
Switch(config)#firewall default permit
```

```
Switch(config)#interface ethernet 1/0/10
```

```
Switch(Config-If-Ethernet1/0/10)#ipv6 access-group 600 in
```

```
Switch(Config-If-Ethernet1/0/10)#exit
```

```
Switch(config)#exit
```

配置结果：

```
Switch#show firewall
```

```
Firewall Status: Enable.
```

```
Firewall Default Rule: Permit.
```

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

```
Ipv6 access-list 600(used 1 time(s))
```

```
ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
```

```
ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source
```

```
Switch #show access-group interface ethernet 1/0/10
```

```
interface name:Ethernet1/0/10
```

```
IPv6 Ingress access-list used is 600, traffic-statistics Disable.
```

案例 5:

用户有以下配置需求：交换机的端口 1, 2, 5, 7 属于 Vlan100，管理员不希望 IP 地址为 192.168.0.1 的设备接入到这几个端口。

配置更改：

1. 创建相应的 ACL
2. 配置包过滤功能
3. 绑定 ACL 到端口

配置步骤如下：

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

```
Switch (config)#vlan 100
```

```
Switch (Config-Vlan100)#switchport interface ethernet 1/0/1;2;5;7
```

```
Switch (Config-Vlan100)#exit
```

```
Switch (config)#access-list 1 deny host-source 192.168.0.1
```

```
Switch (config)#interface ethernet1/0/1;2;5;7
```

```
Switch (config-if-port-range)#ip access-group 1 in
```

```
Switch (Config-if-Vlan100)#exit
```

配置结果：

```
Switch (config)#show access-group interface vlan 100
```

```
Interface VLAN 100:
```

```
Ethernet1/0/1:   IP Ingress access-list used is 1, traffic-statistics Disable.
```

```
Ethernet1/0/2:   IP Ingress access-list used is 1, traffic-statistics Disable.
```

```
Ethernet1/0/5:   IP Ingress access-list used is 1, traffic-statistics Disable.
```

```
Ethernet1/0/7:   IP Ingress access-list used is 1, traffic-statistics Disable.
```

1.4 ACL排错帮助

- ☞ 对 ACL 中的表项的检查是自上而下的，只要匹配一条表项，对此 ACL 的检查就马上结束。
- ☞ 端口特定方向上没有绑定 ACL 或没有任何 ACL 表项匹配时，才会使用默认规则。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（通过物理接口配置模式或 Vlan 接口配置模式）。
- ☞ 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 IP ACL
 - ◆ 入口 MAC ACL
- ☞ 端口可以成功绑定的 ACL 数目取决于已绑定的 ACL 的内容以及硬件资源限制。
- ☞ 如果 access-list 中包括过滤信息相同但动作矛盾的规则，则其无法绑定到端口并将有报错提示。例如同时配置 permit tcp any-source any-destination 及 deny tcp any-source any-destination。
- ☞ 可以配置 ACL 拒绝某些 ICMP 报文通过以防止“冲击波”等病毒攻击。
- ☞ 如果物理接口的模式为 Trunk，则该端口只能通过物理接口配置模式配置 ACL。
- ☞ 在物理接口配置模式下绑定的 ACL 只能在物理接口配置模式下取消，在 Vlan 接口配置模式下绑定的 ACL 只能在 Vlan 接口模式下取消。
- ☞ 物理接口加入/移出 Vlan 时（Trunk 口除外），该 Vlan 中配置的 ACL 将自动绑定/移除该物理接口；如果目的 Vlan 中配置的 ACL（通过 Vlan 接口配置模式配置）和该端口原有的 ACL 配置（通过物理接口配置模式配置）冲突，将导致端口移动失败。
- ☞ Vlan 中无物理接口时（Trunk 口除外），将删除 ACL 在 Vlan 中的配置，以后如果再有物理端口移入 Vlan，将无 ACL 应用于该物理接口。端口模式转换：access->trunk，将取消通过 Vlan 接口配置模式绑定到该物理接口的 ACL；trunk->access，将 Vlan 1 接口配置的 ACL 绑定到该物理接口，如果绑定失败，端口模式转换将执行失败。

第2章 802.1x配置

说明：

本章所指的三层交换机代表了一般意义下的路由器或运行了路由协议的无线控制产品。

2.1 802.1x介绍

802.1x协议起源于802.11协议，后者是IEEE的无线局域网协议，制订802.1x协议的初衷是为了解决无线局域网用户的接入认证问题。IEEE 802 LAN协议定义的局域网并不提供接入认证，只要用户能接入局域网控制设备（如LAN Switch），就可以访问局域网中的设备或资源。这在早期企业网有线LAN应用环境下并不存在明显的安全隐患。

随着移动办公及驻地网运营等应用的大规模发展，服务提供者需要对用户的接入进行控制和配置。尤其是WLAN的应用和LAN接入在电信网上大规模开展，有必要对端口加以控制以实现用户级的接入控制，802.1x就是IEEE LAN/WAN 委员会为了解决基于端口的网络接入控制（Port-Based Network Access Control）而定义的一个标准，该标准目前已经在无线局域网和以太网中被广泛应用。

“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

2.1.1 802.1x认证体系结构

使用802.1x的系统为典型的Client/Server体系结构，包括三个实体，如下图所示，分别为：Supplicant system（客户端）、Authenticator system（接入控制单元）以及Authentication server system（认证服务器）。

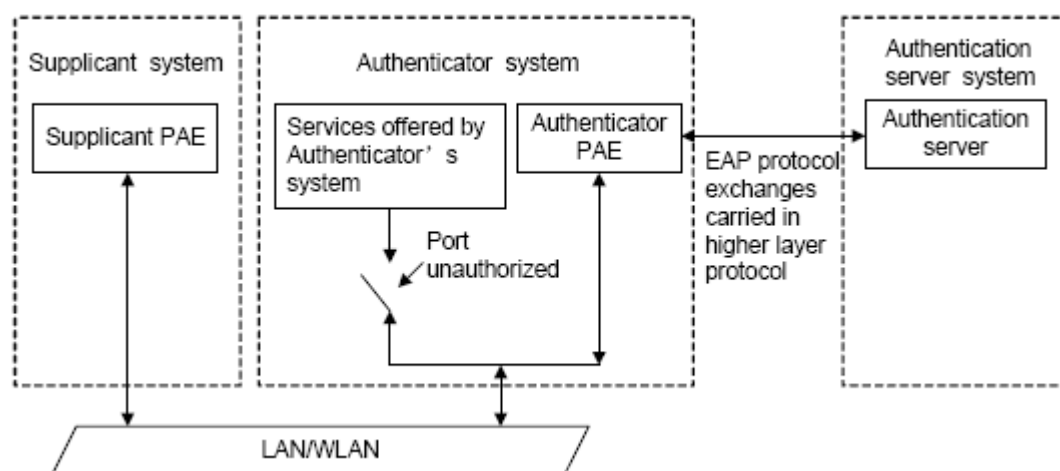


图 2-1 802.1x 认证体系结构

客户端是位于局域网段一端的一个实体，由该链路另一端的接入控制单元对其进行

认证。客户端一般为一个用户终端设备，用户通过启动客户端软件发起802.1x认证。客户端必须支持EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）。

- ✎ 接入控制单元是位于局域网段一端的另一个实体，对所连接的客户端进行认证。接入控制单元通常为支持802.1x 协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- ✎ 认证服务器是为接入控制单元提供认证服务的实体。认证服务器用于实现对用户进行认证、授权和计费，通常为RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。该服务器可以存储有关用户的信息。包括用户名、密码以及其它参数，例如用户所属的VLAN、端口等。

三个实体涉及以下三个基本概念：端口 PAE、受控端口和受控方向。

1. PAE

PAE（Port Access Entity，端口访问实体）是 802.1x 认证机制中负责执行算法和协议操作的实体。

- ✎ 客户端PAE负责响应接入控制单元的认证请求，向接入控制单元提交用户的认证信息。客户端PAE也可以主动向接入控制单元发送认证请求和下线请求。
- ✎ 接入控制单元PAE利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果对受控端口的授权/非授权状态进行相应地控制。授权状态是指允许用户访问网络资源；非授权状态是指仅允许EAPOL报文收发，不允许用户访问网络资源。

2. 受控/非受控端口

接入控制单元为客户端提供接入局域网的端口，这个端口被划分为两个逻辑端口：受控端口和非受控端口。

- ✎ 非受控端口始终处于双向连通状态，主要用来传递EAPOL协议帧，保证客户端始终能够发出或接收认证报文。
- ✎ 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。
- ✎ 受控端口和非受控端口是同一端口的两个部分；任何到达该端口的帧，在受控端口与非受控端口上均可见。

3. 受控方向

在非授权状态下，受控端口可以被设置成单向受控或双向受控。

- ✎ 实行双向受控时，禁止帧的发送和接收。
- ✎ 实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

说明：目前，本交换机只支持单向受控。

2.1.2 802.1x工作机制

IEEE 802.1x 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协

议)，来实现客户端、接入控制单元和认证服务器之间认证信息的交换。

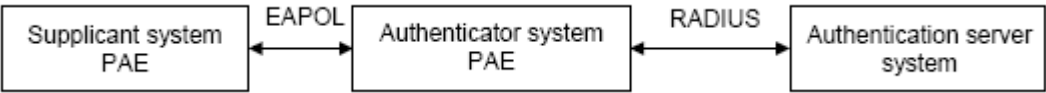


图 2-2 802.1x 认证工作机制

- 在客户端PAE与接入控制单元PAE之间，EAP协议报文使用EAPOL封装格式，直接承载于LAN环境中。
- 在接入控制单元PAE与RADIUS服务器之间，可以使用两种方式来交换信息。一种是EAP协议报文使用EAPOR（EAP over RADIUS）封装格式承载于RADIUS协议中；另一种是EAP协议报文由接入控制单元PAE进行终结，采用包含PAP（Password Authentication Protocol，密码验证协议）或CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）属性的报文与RADIUS服务器进行认证交互。
- 当用户完成认证后，认证服务器会把用户的相关信息传递给接入控制单元，接入控制单元PAE根据RADIUS服务器的认证结果（Accept 或Reject）决定受控端口的授权/非授权状态。

2.1.3 EAPOL消息的封装

1. EAPOL 数据包的格式

EAPOL 是 802.1x 协议定义的一种报文封装格式，主要用于在客户端和接入控制单元之间传送 EAP 协议报文，以允许 EAP 协议报文在 LAN 上传送。在 IEEE 802/Ethernet LAN 环境中，EAPOL 数据包的格式如下图所示，EAPOL 数据包的起始位置是 MAC 帧的 Type/Length 域。

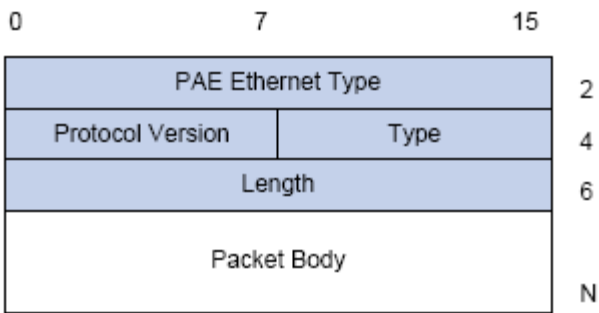


图 2-3 EAPOL 数据包格式

PAE Ethernet Type: 表示协议类型，为 0x888E。

Protocol Version: 表示 EAPOL 数据包的发送方所支持的协议版本号。

Type: 表示 EAPOL 数据包类型，具体类型包括：

- EAP-Packet（值为0x00）：认证信息帧，用于承载EAP报文。该帧能够穿越（Pass through）接入控制单元，在客户端和认证服务器之间传递EAP报文。
- EAPOL-Start（值为0x01）：认证发起帧。
- EAPOL-Logoff（值为0x02）：退出请求帧。
- EAPOL-Key（值为0x03）：密钥信息帧。

- ✎ EAPOL-Encapsulated-ASF-Alert（值为0x04）：用于支持ASF（Alert Standard Forum）的Alerting 消息。该帧用于封装与网管相关信息，例如各种警告信息，由设备端终结。

Length：表示数据长度，也就是“Packet Body”字段的长度，单位为字节。如果为 0，则表示没有后面的数据域。

Packet Body：表示数据内容，根据不同的 Type 有不同的格式。

2. EAP 数据包的格式

当 EAPOL 数据包格式 Type 域为 EAP-Packet 时，Packet Body 为 EAP 数据包结构，如下图所示。

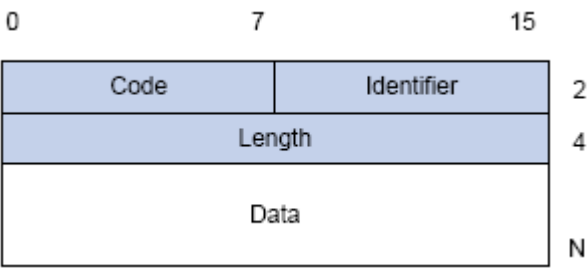


图 2-4 EAP 数据包格式

Code：指明 EAP 数据包的类型，共有 4 种：Request（1）、Response（2）、Success（3）、Failure（4）。

- ✎ Success 和Failure 类型的包没有Data域，相应的Length 域的值4。
- ✎ Request和Response类型数据包的Data域的格式如下图所示。Type为EAP的认证类型，Type data的内容由类型决定。例如，Type值为1 时代表Identity，用来查询对方的身份；Type值为4 时，代表MD5-Challenge，类似于PPP CHAP协议，包含质询消息。

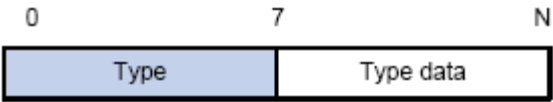


图 2-5 Request 和 Response 类型数据包的 Data 域的格式

Identifier：辅助进行 Request 和 Response 消息的匹配。

Length：EAP 数据包的长度，包含 Code、Identifier、Length 和 Data 域，单位为字节。

Data：EAP 数据包的内容，由 Code 类型决定。

2.1.4 EAP属性的封装

RADIUS 为支持 EAP 认证增加了两个属性：EAP-Message（EAP 消息）和 Message-Authenticator（消息认证码）。RADIUS 协议的报文格式请参见“AAA-RADIUS-HWTACACS 操作”的 RADIUS 协议简介部分。

1. EAP-Message

如图所示，这个属性用来封装 EAP 数据包，类型代码为 79，String 域最长 253 字节，

如果 EAP 数据包长度大于 253 字节，可以对其进行分片，依次封装在多个 EAP-Message 属性中。

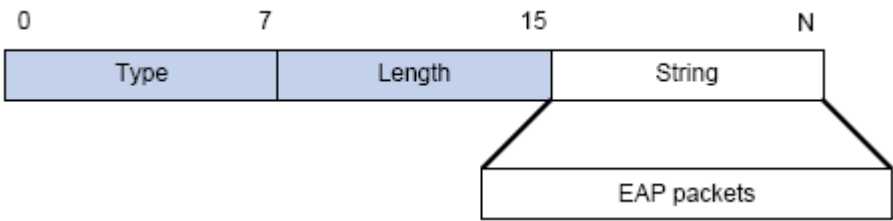


图 2-6 EAP-Message 属性封装

2. Message-Authenticator

如图所示，这个属性用于在使用 EAP、CHAP 等认证方法的过程中，避免接入请求包被窃听。在含有 EAP-Message 属性的数据包中，必须同时也包含 Message-Authenticator，否则该数据包会被认为无效而被丢弃。

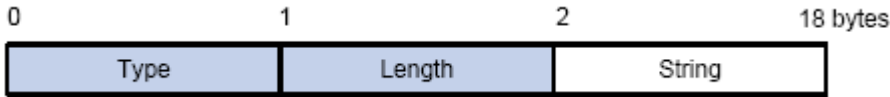


图 2-7 Message-Authenticator 属性

2.1.5 基于 802.1x的Web认证代理功能

原有 802.1x 认证系统的整体思路采用 IEEE 802.1x 认证系统的体系结构、工作机制、基本业务流程，客户端使用专有客户端进行认证，设备端采用二层交换机，认证服务器使用 RADIUS 服务器，认证消息格式采用 EAP 协议。在客户端与认证代理交换机之间使用 EAPOL 封装技术，即将 EAP 报文封装在以太网帧之中进行认证通信；而认证代理交换机与认证服务器间使用 EAPOR 封装格式，即将 EAP 报文承载在 Radius 协议上进行认证通信；也可以由设备端进行中介，而在设备端与 RADIUS 服务器之间通过 RADIUS 协议传送 PAP 协议报文或 CHAP 协议报文。

802.1x 认证系统中，用户为了实现身份认证和网络准入，就必须安装认证客户端软件，通过认证客户端登录触发认证流程，实现与 DCBI 服务器的认证通信。但是现在有些客户工作不希望安装客户端软件，希望可以简单的通过浏览器就实现认证。为了迎合用户新需求，实现认证客户端的平台无关性，我们设计提出了基于原有 802.1x 系统的 Web 认证功能。

Web 认证基本仍采用标准的 802.1x 认证系统，使用浏览器中运行的 Java Applet 替代原有的客户端软件，设备端采用三层交换机，认证服务器使用标准 RADIUS 服务器，认证消息承载在 EAP 报文中进行通信。由于客户端采用 Java Applet 技术，不能发送以太网帧，故而客户端与 web 认证代理交换机的认证通信 EAP 报文不能采用 EAPOL 封装技术，即不能将 EAP 报文封装在以太网帧中发送。因此作为替代采用 EAPOU 技术，即将 EAP 认证报文承载于 UDP 协议之上，实现 web 客户端与 web 认证代理交换机之间的认证通信，而在认证代理交换机与认证服务器之间仍然采用标准的 EAPOR 协议。

2.1.6 802.1x认证方式

认证过程可以由客户端主动发起，也可以由设备端发起。一方面当设备端探测到有未经过认证的用户使用网络时，就会主动向客户端发送 EAP-Request/Identity 报文，发起认证；另一方面客户端可以通过客户端软件向设备端发送 EAPOL-Start 报文，发起认证。

802.1x 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下对这两种认证方式的过程描述，都以客户端主动发起认证为例。

2.1.6.1 EAP中继方式

这种方式是 IEEE 802.1x 标准规定的，将 EAP（扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS 服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator。

EAP 是一个通用的用来传输实际认证协议的认证框架，而不是一个特殊的认证机制。EAP 提供一些公共的功能，并且允许协商所希望的认证机制，这些机制被叫做 EAP 方法（Method）。EAP 的好处就是当一个新的认证协议发展出来的时候，基础的 EAP 机制不需要随着改变，在下图中给出了 EAP 认证方法协议栈。

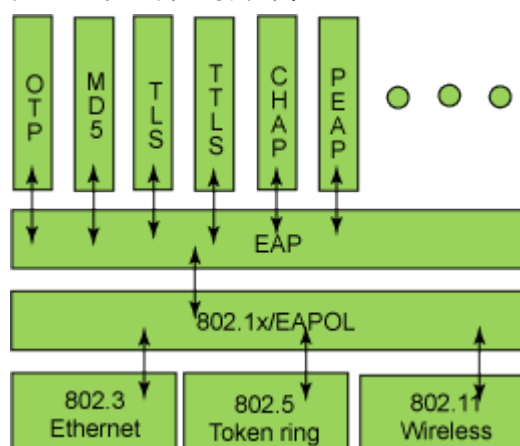


图 2-8 EAP 认证方法协议栈

现在已经开发出 50 种以上的 EAP 认证方法，而各种不同 EAP 认证方法间的差异在于认证机制与密钥管理的不同。其中比较常见的四种 EAP 认证方法包括：

- ☞ **EAP-MD5**
- ☞ **EAP-TLS**（Transport Layer Security，传输层安全）
- ☞ **EAP-TTLS**（Tunneled Transport Layer Security，隧道传输层安全）
- ☞ **PEAP**（Protected Extensible Authentication Protocol，受保护的扩展认证协议）

下面分别介绍这四种 EAP 认证方法。

注意：

- ☞ 交换机作为穿越（Pass-through）接入控制单元，不检查具体 EAP 方法相关的内

容，因而可以支持以上常见的 EAP 方法，并能够支持未来扩展的各种 EAP 认证方法。

- ✎ EAP 中继方式下，如果要采用 EAP-MD5、EAP-TLS、EAP-TTLS 或者 PEAP 这四种认证方法之一，需要保证在客户端和 RADIUS 服务器上选择一致的认证方法。

1. EAP-MD5 认证方法

EAP-MD5 是一个 IETF 开放标准，但提供最少安全，MD5 Hash 函数容易受到字典攻击。

下面给出采用 EAP-MD5 认证方法的基本业务流程，如图所示。

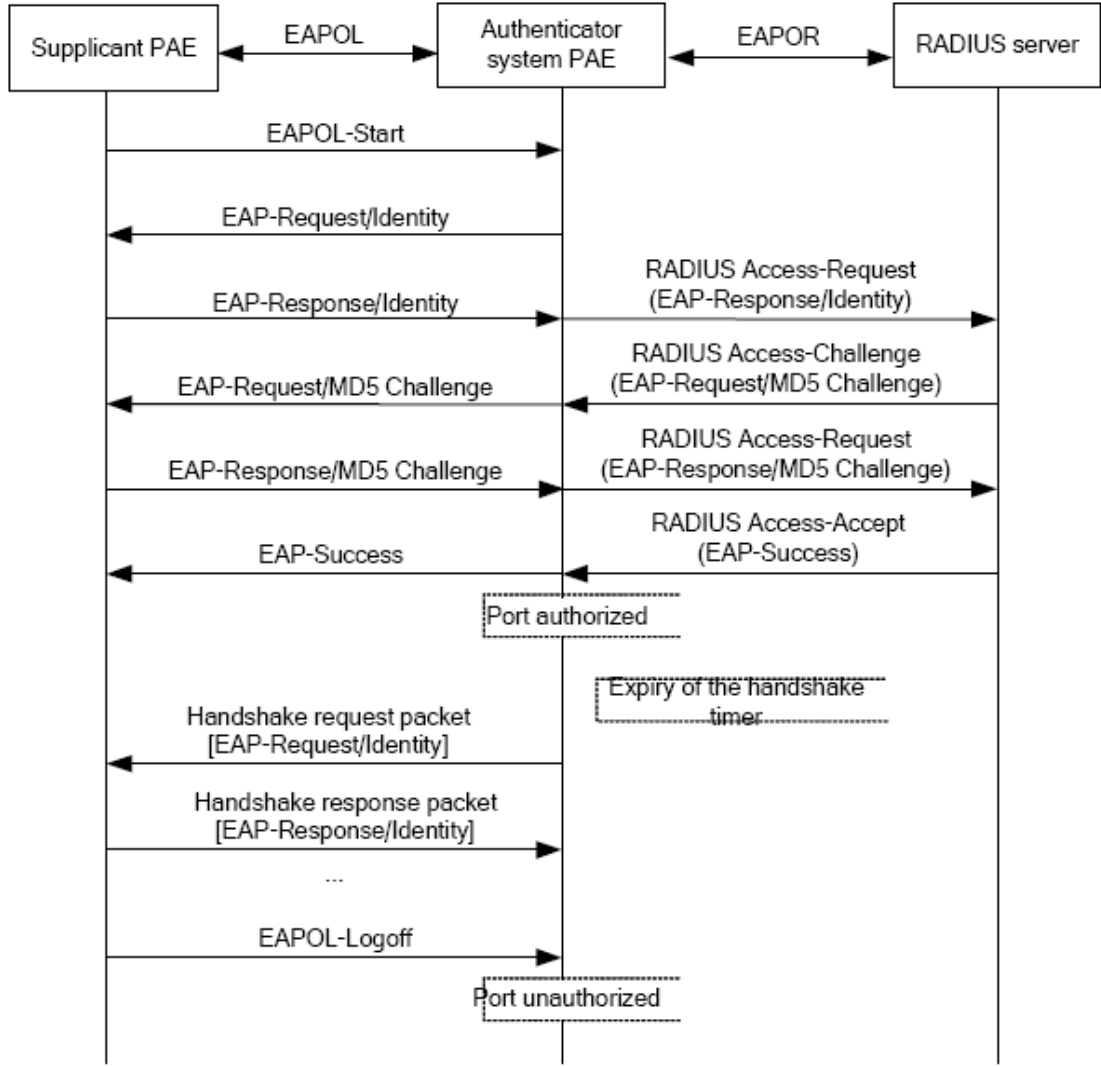


图 2-9 802.1x EAP-MD5 认证流程

2. EAP-TLS 认证方法

EAP-TLS 是由微软公司基于 EAP 和 TLS 协议而提出来的。它使用 PKI 来保护客户端与 Radius 认证服务器之间的身份认证以及生成动态的会话密钥，要求客户端和 Radius 认证服务器都要拥有数字证书以进行双向认证。它是无线局域网最早采纳的 EAP 认证方法。

由于需要每一个用户都要拥有数字证书，因而在实际部署时由于维护困难而很少被使用，但它仍被认为是最安全的 EAP 标准之一，而且广泛地被无线局域网硬件和软件制造厂商所支持。

下面给出采用 EAP-TLS 认证方法的基本业务流程，如图所示。

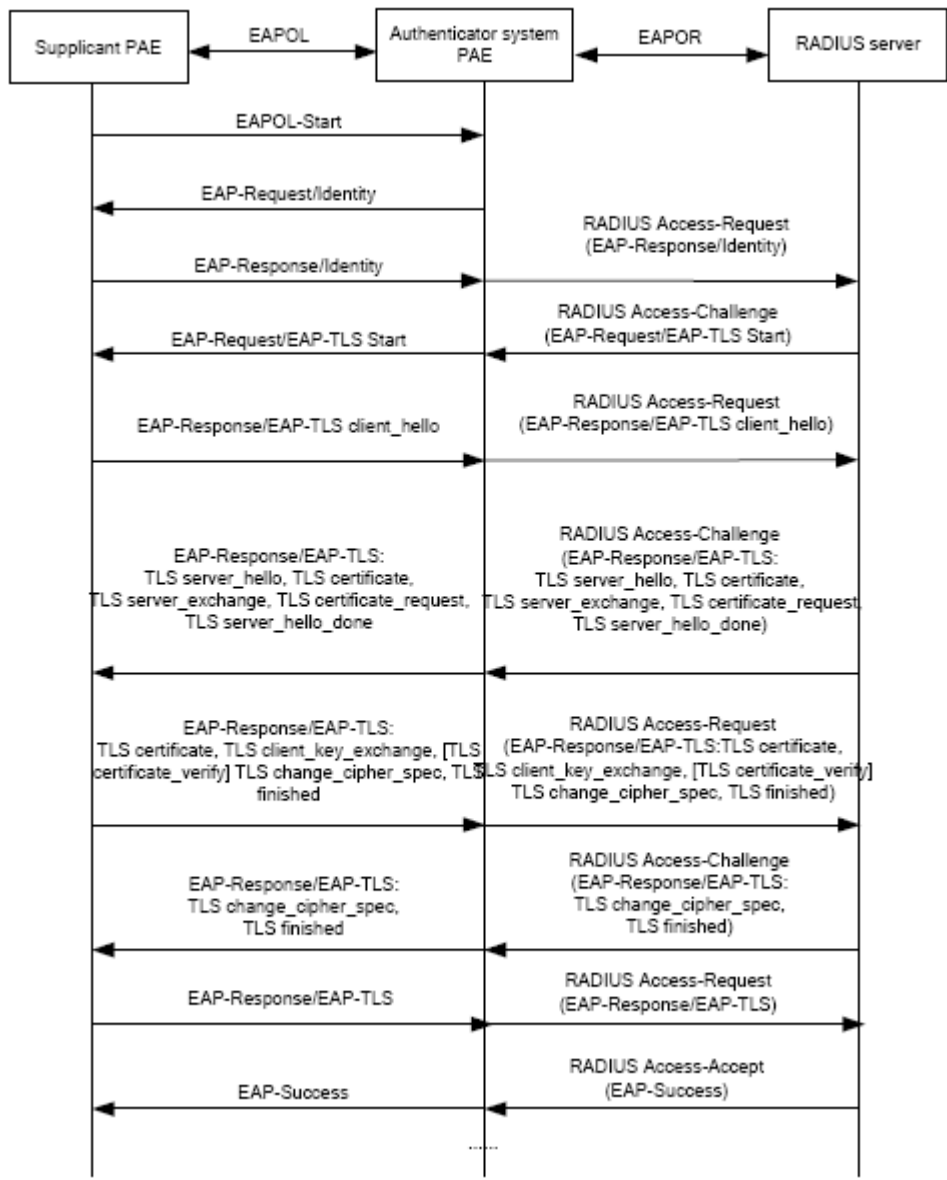


图 2-10 802.1x EAP-TLS 认证流程

3. EAP-TTLS 认证方法

EAP-TTLS 是由 Funk Software 和 Certicom 合作开发的。它可以提供 EAP-TLS 相同的认证强度，但不要求每个用户都要拥有数字证书，而只要求 Radius 认证服务器要拥有数字证书。用户身份的验证是通过密码来进行的，该密码是在利用认证服务器的证书所建立的一个安全的加密的隧道中传输。在 TTLS 隧道内部可以转发任意类型的认证请求，例如 EAP、PAP、MS-CHAPV2 等。

4. PEAP 认证方式

EAP-PEAP 是由 Cisco、微软和 RSA Security 联合提出的开放标准的建议。它早已被运用在产品中，而且提供很好的安全。它在协议设计和安全性方面与 EAP-TTLS 相似，只需要一份服务器端的 PKI 证书来建立一个安全的 TLS 隧道以保护用户认证。

下面给出采用 PEAP 认证方法的基本业务流程，如图所示。

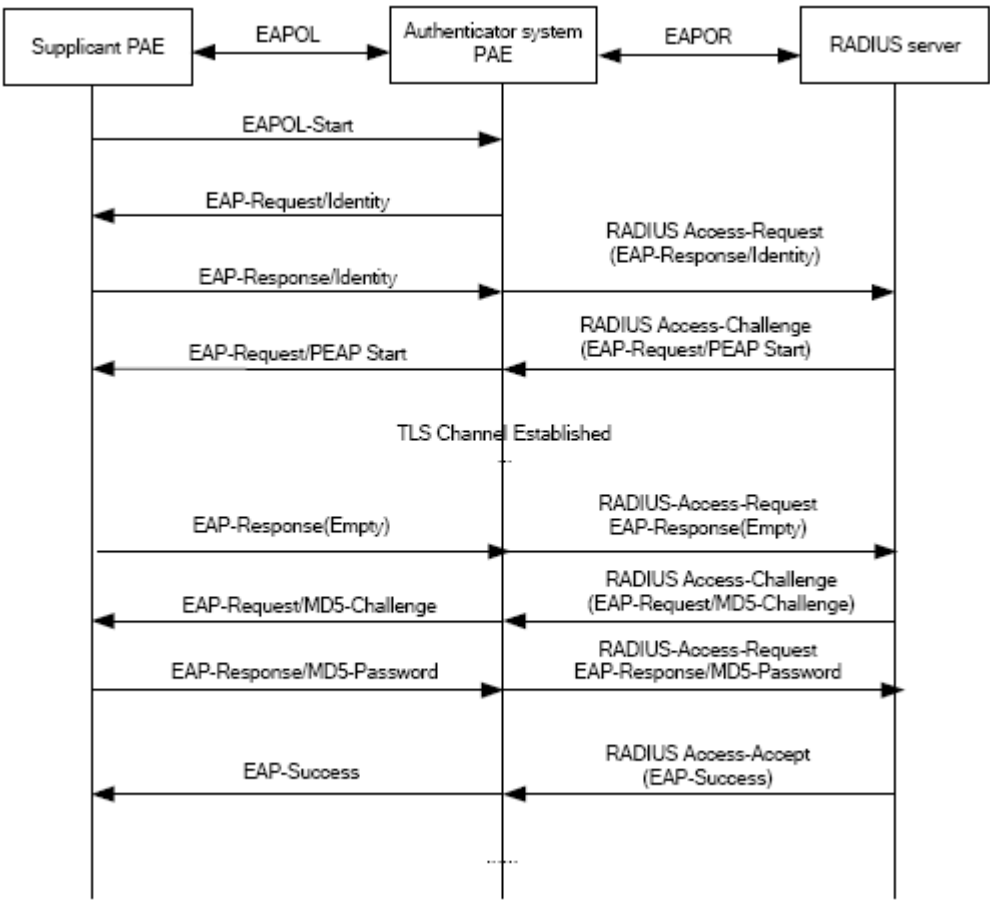


图 2-11 802.1x PEAP 认证流程

2.1.6.2 EAP终结方式

这种方式将 EAP 报文在接入控制单元终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费。基本业务流程如下图所示。

对于 EAP 终结方式，接入控制单元与 RADIUS 服务器之间可以采用 PAP 或者 CHAP 认证方法。以下以 CHAP 认证方法为例介绍基本业务流程，如图所示。

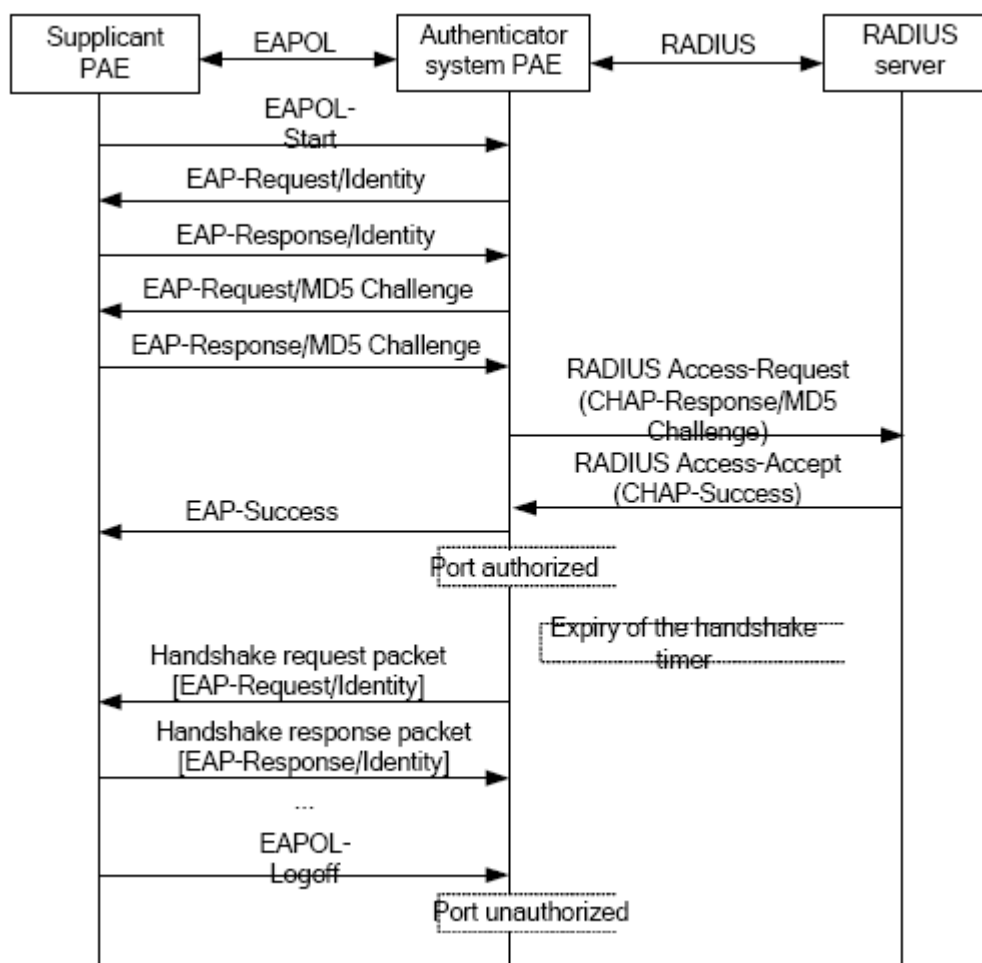


图 2-12 802.1x EAP 终结方式认证流程

EAP 终结方式与 EAP 中继方式的认证流程相比，不同之处在于用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后接入控制单元会把用户名、随机加密字和客户端加密后的密码信息一起送给 RADIUS 服务器，进行相关的认证处理。

2.1.7 802.1x的扩展和优化

设备在 802.1x 的 EAP 中继方式和 EAP 终结方式的实现中，不仅支持协议所规定的端口接入认证方式，还对其进行了扩展、优化：

- (1) 支持一个物理端口下挂接多个用户的应用场合；
- (2) 接入控制方式（即对用户的认证方式）可以采用基于端口、基于MAC和基于用户（IP地址+MAC地址+端口）三种方式：
 - 当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
 - 当采用基于MAC方式时，对于同一物理端口下的所有接入用户均需要单独认证，只有通过了认证的用户才能够接入网络，没有通过认证的用户不能接入网络。当某个用户下线时，也只有该用户无法使用网络。

- 当采用基于用户（IP地址+MAC地址+端口）方式时，它允许用户在认证之前就能够访问有限资源。对基于用户的接入控制方式，存在标准控制与高级控制两种类型：基于用户的标准控制类型不对有限资源的访问进行限制，该端口下的所有用户在没有经过认证之前都可以访问有限资源，当认证通过后可以访问所有资源；但基于用户的高级控制类型会对有限资源的访问进行限制，在该端口下只有特定用户在没有经过认证之前能够访问有限资源，当这些用户认证通过后可以访问所有资源。

注意：当使用私有的客户端时，推荐采用基于用户的高级接入控制方式，采用这种方式可以有效地防止 ARP 欺骗。

交换机最大认证用户数可以达到 4000 人，推荐使用认证用户数不超过 2000 人。

2.1.8 VLAN分配特性

1. Auto VLAN

Auto VLAN 特性可以使 RADIUS 服务器根据用户信息和用户接入设备信息来动态改变接入端口所属的 VLAN。当 802.1x 用户在服务器上通过认证时，RADIUS 服务器会把授权信息传送给设备端。如果 RADIUS 服务器上配置了下发 VLAN 功能，则在 Access-Accept 报文中应当含有以下属性：

4. Tunnel-Type = VLAN (13)
5. Tunnel-Medium-Type = 802 (6)
6. Tunnel-Private-Group-ID = VLANID

这里的 VLANID 是指 VLAN 的 VID，取值范围为 1~4094。例如 Tunnel-Private-Group-ID = 30 表示 VLAN 30。

当交换机接收到下发的 Auto VLAN 信息后，当前 Access 端口离开用户配置的 VLAN 并加入 Auto VLAN 中。

Auto VLAN 并不改变端口的配置，也不影响端口的配置。但是，Auto VLAN 的优先级高于用户配置的 VLAN，即通过认证后起作用的 VLAN 是 Auto VLAN，用户配置的 VLAN 在用户下线后生效。

说明：目前 Auto VLAN 只能在基于端口的接入控制方式，以及链路类型为 Access 类型的端口上生效。

2. Guest VLAN

Guest VLAN 特性用来允许未认证用户访问某些特定资源。

用户认证端口在通过 802.1x 认证之前属于一个缺省 VLAN（即 Guest VLAN），用户访问该 VLAN 内的资源不需要认证，但此时不能够访问其他网络资源；认证成功后，端口离开 Guest VLAN，用户可以访问其他的网络资源。

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）。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。

开启 802.1x 特性并正确配置 Guest VLAN 后，当设备从某一端口发送触发认证报文（EAP-Request/Identity）超过设定的最大次数而没有收到客户端的任何回应报文时，与 Auto VLAN 类似，该端口将被加入到 Guest VLAN 内。此时 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 Guest Vlan 内。

2.2 802.1x配置

802.1x 配置任务序列如下：

1. 使能交换机的 802.1x 功能
2. 配置基于 802.1x 的 web 认证代理全局功能
3. 接入控制单元的属性配置
 - 1) 配置端口的授权状态
 - 2) 配置端口的接入控制方式：基于 MAC 地址还是基于端口
 - 3) 配置交换机 802.1x 的扩展功能
 - 4) 配置端口的 IPv6 透传功能
4. 与 Supplicant (用户接入设备)相关的属性配置（可选）

1.使能交换机的 802.1x 功能

命令	解释
全局配置模式	
dot1x enable no dot1x enable	使能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。
dot1x privateclient enable no dot1x privateclient enable	使能交换机强制客户端软件使用私有 802.1x 认证报文格式；本命令的 no 操作为关闭该功能，允许客户端软件使用标准 802.1x 认证报文格式。
dot1x user free-resource <prefix> <mask> no dot1x user free-resource	设置用户能够访问的有限资源；本命令的 no 操作为删除有限资源。

dot1x unicast enable	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。
no dot1x unicast enable	

2. 配置基于 802.1x 的 web 认证代理全局功能

命令	解释
全局配置模式	
dot1x web authentication enable no dot1x web authentication enable	全局启动基于 802.1x 的 web 认证代理局功能；本命令的 no 操作为关闭该功能。
dot1x web redirect <URL> no dot1x web redirect	在交换机上配置 Web 重定向的 HTTP 服务器地址，不支持域名解析，所以不要配置域名；本命令的 no 操作清除 Web 重定向的 HTTP 服务器地址。

3. 接入控制单元的属性能配置

1) 配置端口的授权状态

命令	解释
端口配置模式	
dot1x port-control {auto force-authorized force-unauthorized} no dot1x port-control	设置端口的 802.1x 授权状态，本命令的 no 操作用来恢复缺省配置。

2) 配置端口的接入控制方式

命令	解释
端口配置模式	
dot1x port-method {macbased portbased webbased userbased {standard advanced}} no dot1x port-method	设置端口的接入控制方式；本命令的 no 操作用来恢复缺省的接入控制方式。
dot1x max-user macbased <number> no dot1x max-user macbased	设置指定端口最多允许接入的用户数；本命令的 no 操作为恢复缺省的最多允许 1 个用户。
dot1x max-user userbased <number> no dot1x max-user userbased	设置指定端口最多允许接入的用户数，用于端口接入控制方式为 userbased 的情况；本命令的 no 操作为恢复缺省的最多允许 10 个用户。
dot1x guest-vlan <vlanID> no dot1x guest-vlan	设置指定端口的 guest vlan；本命令的 no 操作为删除 guest vlan。

dot1x portbased mode single-mode	配置基于 portBase 认证方式的单一用户模式；本命令的 no 操作为关闭该功能。
no dot1x portbased mode single-mode	

3) 配置交换机 802.1x 的扩展功能

命令	解释
全局配置模式	
dot1x macfilter enable no dot1x macfilter enable	打开交换机 802.1x 的地址过滤功能；本命令的 no 操作为关闭 802.1x 的地址过滤功能。
dot1x macbased port-down-flush no dot1x macbased port-down-flush	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。
dot1x accept-mac <mac-address> [interface <interface-name>] no dot1x accept-mac <mac-address> [interface <interface-name>]	添加 802.1x 的地址过滤表的表项；本命令的 no 操作为删除 802.1x 的地址过滤表的表项。
dot1x eapor enable no dot1x eapor enable	打开交换机 EAP 中继的认证方式；本命令的 no 操作为采用 EAP 本地终结的认证方式。

4) 配置端口的 IPv6 透传功能

命令	解释
端口配置模式	
dot1x ipv6 passthrough no dot1x ipv6 passthrough	使能交换机端口的 IPv6 透传功能，用于端口接入控制方式为 userbased 的情况；本命令的 no 操作为关闭该功能。
dot1x web authentication ipv6 passthrough no dot1x web authentication ipv6 passthrough	打开交换机端口的 IPv6 透传功能，用于端口接入控制方式为 webbased 的情况；本命令的 no 操作为关闭该功能。

4. 与 Supplicant (用户接入设备)相关的属性配置

命令	解释
全局配置模式	
dot1x max-req <count> no dot1x max-req	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 操作用来恢复缺省值。

dot1x re-authentication no dot1x re-authentication	设置允许对 supplicant 进行周期性重认证；本命令的 no 操作用来关闭该功能。
dot1x timeout quiet-period <seconds> no dot1x timeout quiet-period	设置在端口认证失败后保持静默状态的时间；本命令的 no 操作用来恢复缺省值。
dot1x timeout re-authperiod <seconds> no dot1x timeout re-authperiod	设置交换机对 supplicant 重新认证的时间间隔；本命令的 no 操作用来恢复缺省值。
dot1x timeout tx-period <seconds> no dot1x timeout tx-period	设置交换机对 supplicant 重发 EAP-request/identity 帧的时间间隔；本命令的 no 操作用来恢复缺省值。
dot1x re-authenticate [interface <interface-name>]	设置对所有端口或某个指定端口进行 802.1x 重认证（不须等待超时）。

2.3 802.1x应用举例

2.3.1 Guest Vlan应用举例

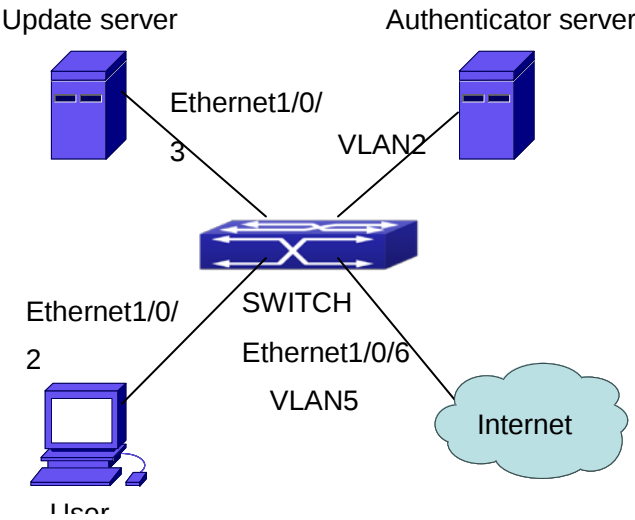


图 2-13: Guest VLAN 网络拓扑结构

如图 2-13 所示，1 台交换机通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器。User 接入交换机的端口 Ethetnet1/0/2 下，端口 Ethernet 1/0/2 在 VLAN100 内；认证服务器在 VLAN2 内；Update Server 是用于客户端软件下载和升级的服务器，在 VLAN10 内；交换机连接 Internet 网络的端口 Ethernet 1/0/6 在 VLAN5 内。

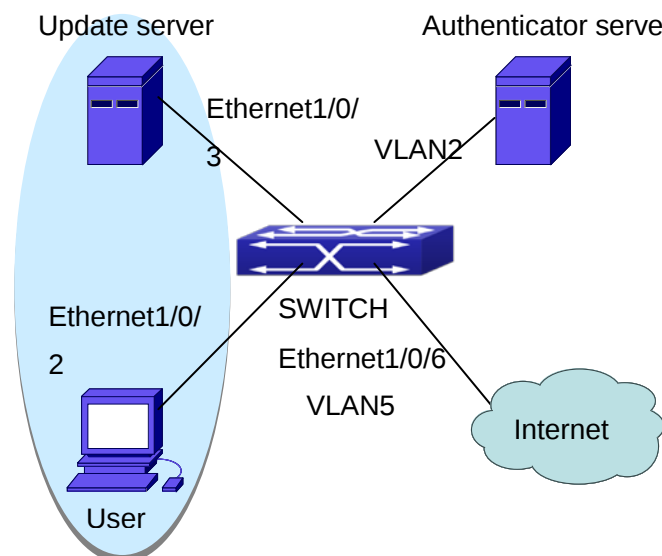


图 2-14: 用户加入 Guest VLAN

如图 2-14 所示，在交换机端口 Ethernet1/0/2 上开启 802.1x 特性，并配置 VLAN10 为该端口 Guest VLAN，当用户没有认证或者认证失败时，端口 Ethernet1/0/2 被加入到 VLAN10 中，用户可以访问 Update Server。

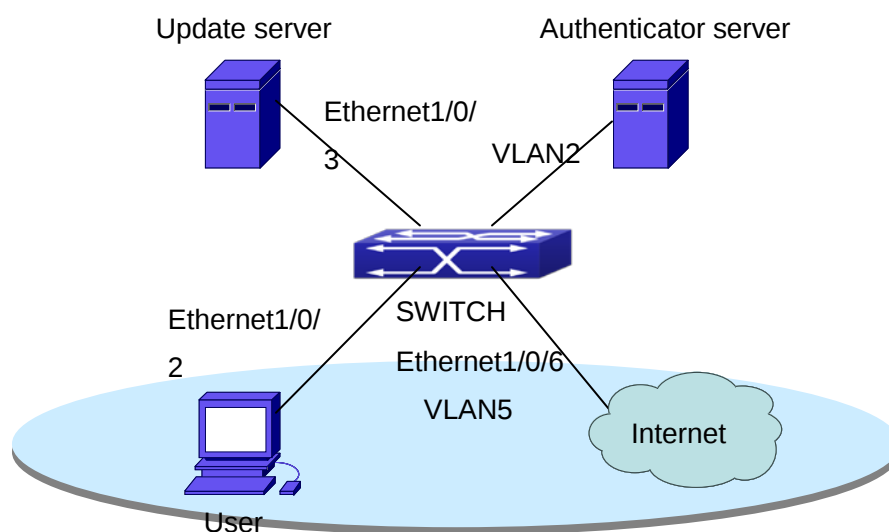


图 2-15: 用户上线，VLAN 下发

如图 2-15 所示，当用户认证成功上线，认证服务器下发 VLAN5，此时，用户和端口 Ethernet1/0/6 都在 VLAN5 内，用户可以访问 Internet。

配置步骤如下：

配置 RADIUS 服务器。

```
Switch(config)#radius-server authentication host 10.1.1.3
```

```
Switch(config)#radius-server accounting host 10.1.1.3
```

```
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable

# 创建 VLAN100。
Switch(config)#vlan 100

# 使能全局 802.1x 功能。
Switch(config)#dot1x enable

# 使能端口 Ethernet1/0/2 上的 802.1x 功能。
Switch(config)#interface ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#dot1x enable

# 配置端口的链路类型为 access 模式。
Switch(Config-Ethernet1/0/2)#switch-port mode access

# 配置端口上接入控制方式为 portbased。
Switch(Config-Ethernet1/0/2)#dot1x port-method portbased

# 配置端口上进行接入控制的模式为 auto。
Switch(Config-Ethernet1/0/2)#dot1x port-control auto

# 配置端口 Guest VLAN 为 100。
Switch(Config-Ethernet1/0/2)#dot1x guest-vlan 100
Switch(Config-Ethernet1/0/2)#exit
```

通过命令 **show running-config** 或者 **show interface ethernet 1/0/2** 可以查看 Guest VLAN 配置情况。在没有用户上线、用户认证失败或用户成功下线等情况下发送触发认证报文（EAP-Request/Identity）超过设定的最大次数时，通过命令 **show vlan id 100** 可以查看端口配置的 Guest VLAN 是否生效。

2.3.2 802.1x与IPv4 Radius应用举例

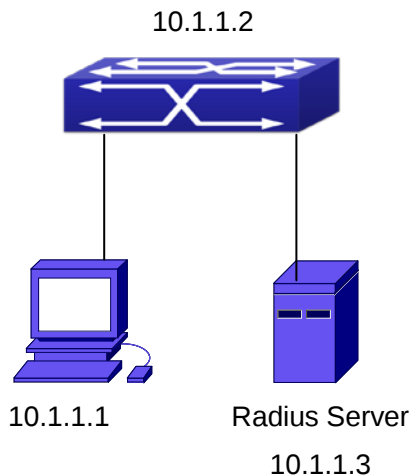


图 2-16 IEEE802.1x 配置举例拓扑图

计算机连接到交换机的端口 Ethernet1/0/2 上，端口 Ethernet1/0/2 开启 IEEE802.1x 认证功能，接入方式采用缺省的基于 MAC 地址认证方式。交换机的 IP 地址设置为 10.1.1.2，并将除端口 Ethernet1/0/2 以外的任意一个端口与 RADIUS 认证服务器相连接，RADIUS 认证服务器的 IP 地址设置为 10.1.1.3，认证、计费端口为缺省端口 1812 和端口 1813。计算机上安装 IEEE802.1x 认证客户端软件，并通过使用此软件来实现 IEEE802.1x 认证。

配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-Ethernet1/0/2)#dot1x enable
Switch(Config-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-Ethernet1/0/2)#exit
```

2.3.3 802.1x与IPv6 Radius应用举例

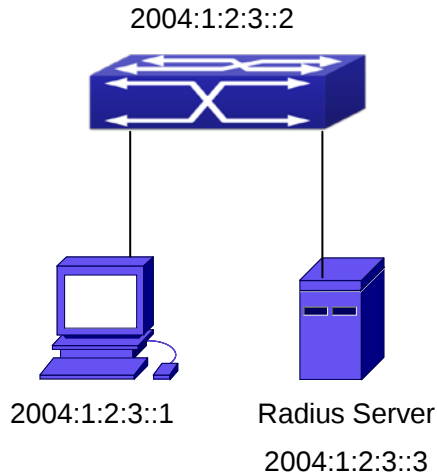


图 2-17 IPv6 Radius 配置举例拓扑图

计算机连接到交换机的端口 1/0/2 上，端口 1/0/2 开启 IEEE802.1x 认证功能，接入方式采用缺省的基于 MAC 地址认证方式。交换机的 IP 地址设置为 2004:1:2:3::2，并将除端口 1/0/2 以外的任意一个端口与 RADIUS 认证服务器相连接，RADIUS 认证服务器的 IP 地址设置为 2004:1:2:3::3，认证、计费端口为缺省端口 1812 和端口 1813。计算机上安装 IEEE802.1x 认证客户端软件，并通过使用此软件来实现 IEEE802.1x 认证。

配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-lf-Ethernet1/0/2)#dot1x enable
Switch(Config-lf-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-lf-Ethernet1/0/2)#exit
```

2.3.4 基于 802.1x 的 Web 认证代理应用举例

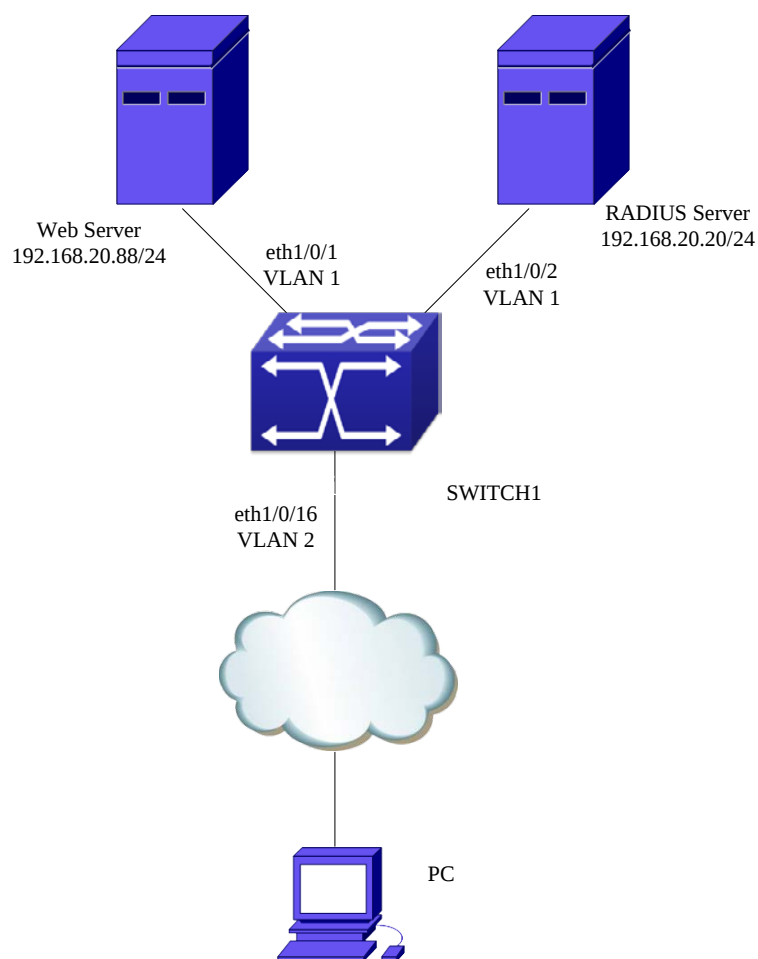


图 2-18 基于 802.1x 的 Web 认证典型配置案例

在上述网络拓扑图中，SWITCH1 的端口 Ethernet1/0/1 与 Web 服务器（IP 地址为 192.168.20.20/24）相连，SWITCH1 的端口 Ethernet1/0/2 与 RADIUS 认证服务器（IP 地址为 192.168.20.88/24，认证端口为 1812）相连，PC 通过一团不可知的网络云与 SWITCH1 的端口 Ethernet1/0/16 相连。Web 服务器和认证服务器处于 VLAN 1 中，PC 处于 VLAN 2 中。可通过下面的配置启动基于 802.1x 的 Web 认证。重认证机制默认是关闭的，要打开重认证功能要执行相应的 802.1x 配置命令。

SWITCH1 配置任务序列：

```
Switch(config)#dot1x enable
```

```
Switch(config)#dot1x web authentication enable
```

```
Switch(config)#dot1x web redirect http://192.168.20.20/WebSupplicant/
```

```
Switch(config)#interface ethernet 1/0/16
```

```
Switch(Config-If-Ethernet1/0/16)#dot1x enable
```

```
Switch(Config-If-Ethernet1/0/16)#dot1x port-method webbased
```

2.4 802.1x排错帮助

用户在使用 802.1x 时,通常会遇到端口无法配置 802.1x;或者 802.1x 认证状态为 **auto**,用户运行 802.1x 的 **supplicant** 软件后,端口仍不能改变为认证通过状态的情况。可能的原因及解决建议如下:

- ☞ 如果出现端口无法配置 802.1x 的情况,请检查交换机的认证端口是否运行了端口 **mac** 绑定,或者端口已经配置为聚合端口。如果要打开端口的 802.1x 认证功能,则必须关闭该端口下的上述功能。
- ☞ 如果交换机配置正确,但认证仍无法通过,请检查交换机与 **RADIUS** 服务器,交换机与 802.1x 客户机之间是否相互连通;检查交换机端口 **VLAN** 的配置。
- ☞ 通过查看 **RADIUS** 服务器的事件日志,判断问题的起因。在事件日志中对登录不成功的不仅有记录还有不成功原因的提示。如事件日志显示 **authenticator** 的登录口令不对,则修改 **radius-server key** 参数;如果事件日志中显示没有该 **authenticator**,则需在 **RADIUS** 服务器中增加该 **authenticator**;如事件日志中提示没有该登录用户,说明用户的登录名和口令有误,输入正确的用户名和口令。
- ☞ 基于 802.1x 的 **Web** 认证代理默认是关闭的。打开基于 802.1x 的 **Web** 认证代理后,可以同时打开调试开关 **debug dot1x** 来查看调试信息。
- ☞ 使用 **show dot1x** 时如果端口的状态显示没有被关闭,只能说明没有被基于 802.1x 的 **Web** 认证代理功能关闭。
- ☞ 基于 802.1x 的 **Web** 认证代理的整个交换机最多能实现 1024 个认证成功用户同时在线,如果超过了此限制,将会返回提示信息。
- ☞ 当用户使用 **Web** 认证无法成功时,检查是否启用了 **dot1x privateclient enable** 命令,若已启用,则需要关闭此私有认证功能。

第3章 端口、VLAN中MAC、IP 数量限制功能配置

3.1 端口、VLAN中MAC、IP 数量限制功能简介

MAC 地址表是标识目的 MAC 地址与交换机端口之间映射关系的表，其 MAC 地址分为静态 MAC 地址和动态 MAC 地址。静态 MAC 地址由用户配置，具有最高优先级（不能被动态 MAC 地址覆盖）且永久生效；动态 MAC 地址由交换机在转发数据帧的过程中学习，且在有限时间内生效。当交换机接收到需要转发的数据帧时，首先学习数据帧的源 MAC 地址，与接收端口建立映射关系；然后根据目标 MAC 地址查询 MAC 地址表，如果命中相关表项，交换机将数据帧从相应端口转发；否则，交换机将数据帧在其所属 VLAN 内广播。

通常交换机支持静态配置和动态学习 MAC 地址的功能，每个端口可以静态配置和动态学习多个 MAC 地址，从而实现端口之间已知 MAC 地址数据流的转发。当 MAC 地址老化后，则进行广播处理。在我们目前的交换机中，端口上对 MAC 地址的数量没有限制，允许一个端口配置或者学习多个 MAC 地址，直到硬件表项填满为止。为了限制端口过量的 MAC 地址，我们需要限制端口的 MAC 地址数量。

对于每一个 INTERFACE VLAN 中的 IP 数量也没有限制，IP 数量限制也就是接口上用户数量的限制，也就是 ARP、ND 表项的限制，这些表项没有相关的配置命令可以控制下发的数量。为了提高产品的安全性能和可控性，我们需要将端口上的 MAC 地址的数量和每个 INTERFACE VLAN 中 ARP、ND 数量进行控制，端口只允许配置的最大数量的动态 MAC 地址存在。每一个 VLAN 上的用户数量不能超过配置允许的用户数量。

对 MAC、ARP 表项进行限制可以在一定程度上防止 DOS 攻击。当恶意用户频繁发动 MAC、ARP 欺骗时，很容易把交换机的 MAC、ARP 表项填满，从而导致 DOS 攻击的发生。对数量进行限制，可以预防 DOS 攻击的发生。

综上节所述，开发端口、VLAN 中的 MAC、IP 数量限制的功能具有重大意义。交换机将可以通过配置命令控制端口的 MAC 地址的数量，同时可以通过配置命令控制端口和 VLAN 中的 ARP、ND 表项的数量。

端口动态 MAC、IP 数量的限制：

- 1.动态 MAC 数量限制，对于交换机已经动态学习到的 MAC 地址，如果大于等于允许学习的最大动态 MAC 数量时，则关闭该端口的 MAC 学习功能，如果少于允许学习的最大动态 MAC 数量时，这时仍然可以继续学习。
- 2.动态 IP 数量限制，对于交换机已经动态学习到的 ARP、ND，如果大于等于允许学习的最大动态 ARP、ND 数量时，则可以关闭该端口的 ARP、ND 学习功能，如果少于允许学习的最大动态 ARP、ND 数量时，这时仍然可以继续学习。

接口 MAC、ARP、ND 数量的限制：

- 1.动态 MAC 数量限制，对于交换机 VLAN 中已经动态学习到的 MAC 地址，如果大于

允许学习的最大动态 MAC 数量时,则可以关闭该 VLAN 中所有端口的 MAC 学习功能,如果少于允许学习的最大动态 MAC 数量时,这时 VLAN 中所有端口仍然可以继续学习。(特殊端口除外)

2.动态 IP 数量限制,对于交换机已经动态学习到的 ARP、ND,如果大于等于允许学习的最大动态 ARP、ND 数量时,则该 VLAN 不会学习新的 ARP、ND,如果少于允许学习的最大动态 ARP、ND 数量时,这时仍然可以继续学习。

3.2 端口、VLAN中MAC、IP数量限制功能配置任务序列

- 1) 启动端口上 MAC、IP 数量限制功能
- 2) 启动 VLAN 中 MAC、IP 数量限制功能
- 3) 配置查询动态 MAC 的超时时间
- 4) 配置端口违背模式
- 5) 显示和调试端口上 MAC、IP 数量限制相关信息

- 1) 启动端口上 MAC、IP 数量限制功能

命令	解释
端口配置模式	
switchport mac-address dynamic maximum <value> no switchport mac-address dynamic maximum	启动和关闭端口 MAC 数量限制功能
switchport arp dynamic maximum <value> no switchport arp dynamic maximum	启动和关闭端口 ARP 数量限制功能
switchport nd dynamic maximum <value> no switchport nd dynamic maximum	启动和关闭端口 ND 数量限制功能

- 2) 启动 VLAN 中 MAC、IP 数量限制功能

命令	解释
VLAN 配置模式	
vlan mac-address dynamic maximum <value> no vlan mac-address dynamic maximum	启动和关闭 VLAN 中 MAC 数量限制功能
接口配置模式	
ip arp dynamic maximum <value> no ip arp dynamic maximum	启动和关闭 VLAN 中 ARP 数量限制功能

ipv6 nd dynamic maximum <value>	启动和关闭 VLAN 中 NEIGHBOR 数量限制功能
no ipv6 nd dynamic maximum	

3) 配置查询动态 MAC 的超时时间

命令	解释
全局配置模式	
mac-address query timeout <seconds>	设置定时查询动态 MAC 的超时时间

4) 配置端口违背模式

命令	解释
端口配置模式	
switchport mac-address violation {protect shutdown} [recovery <5-3600>] no switchport mac-address violation	设置端口违背模式；本命令的 no 操作为恢复违背模式为 protect。

5) 显示和调试端口上 MAC、IP 数量限制相关信息

命令	解释
特权配置模式	
show mac-address dynamic count {vlan <vlan-id> interface ethernet <portName> }	显示相应端口、VLAN 中的动态 MAC 数量
show arp-dynamic count {vlan <vlan-id> interface ethernet <portName> }	显示相应端口、VLAN 中的动态 ARP 数量
show nd-dynamic count {vlan <vlan-id> interface ethernet <portName> }	显示相应端口、VLAN 中的动态 NEIGHBOR 数量
debug switchport mac count no debug switchport mac count	端口 MAC 数量限制时，各种调试信息
debug switchport arp count no debug switchport arp count	端口 ARP 数量限制时，各种调试信息
debug switchport nd count no debug switchport nd count	端口 NEIGHBOR 数量限制时，各种调试信息
debug vlan mac count no debug vlan mac count	VLAN 中 MAC 数量限制时，各种调试信息
debug ip arp count no debug ip arp count	VLAN 中 ARP 数量限制时，各种调试信息

debug ipv6 nd count no debug ipv6 nd count	VLAN 中 NEIGHBOR 数量限制时，各种调试信息
---	------------------------------

3.3 端口、VLAN 中 MAC、IP 数量限制功能典型案例

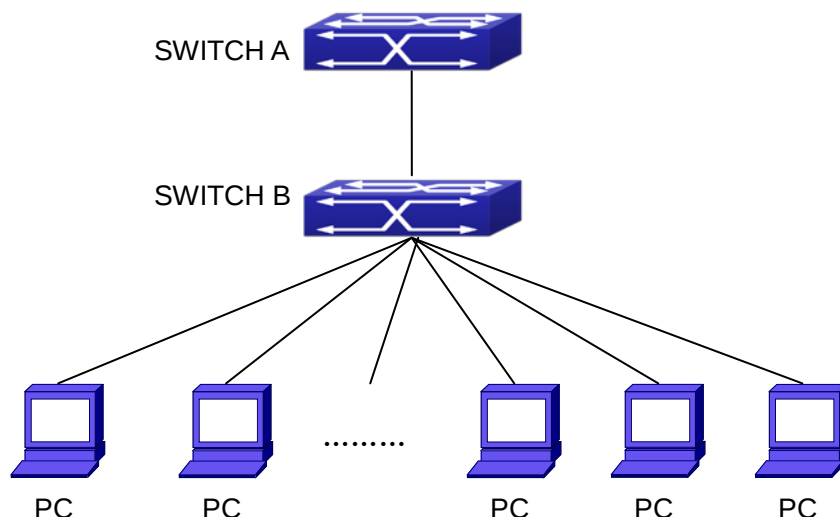


图 3-1 端口、VLAN 中 MAC、IP 数量限制典型配置案例

如上图所示的网络拓扑中, SWITCH B 下面链接很多 PC 用户, 在没有启动端口 MAC、VLAN 中 IP 数量限制功能前, 在系统硬件允许的情况下, SWITCH A, SWITCH B 可以得到所有 PC 的 MAC、ARP、ND 表项, 对 MAC、ARP 表项进行限制可以在一定程度上防止 DOS 攻击。当恶意用户频繁发动 MAC、ARP 欺骗时, 很容易把交换机的 MAC、ARP 表项填满, 从而导致 DOS 攻击的发生。对 MAC、ARP、ND 表项数量进行限制, 可以预防 DOS 攻击的发生。

设置 SWITCH A 端口 Ethernet1/0/1 上最大可以学习 20 个动态 MAC 地址、20 个动态 ARP 地址、10 个 NEIGHBOR 表项, VLAN 1 中允许 30 个动态 MAC 地址, 30 个动态 ARP 地址、20 个 NEIGHBOR 表项。

SWITCH A 配置任务序列:

```
Switch (config)#interface ethernet 1/0/1
```

```
Switch (Config-If-Ethernet1/0/1)#switchport mac-address dynamic maximum 20
```

```
Switch (Config-If-Ethernet1/0/1)#switchport arp dynamic maximum 20
```

```
Switch (Config-If-Ethernet1/0/1)#switchport nd dynamic maximum 10
```

```
Switch (Config-if-Vlan1)#vlan mac-address dynamic maximum 30
```

3.4 端口、VLAN 中 MAC、IP 数量限制功能排错帮助

端口、VLAN 中 MAC、IP 数量限制功能默认情况下是关闭的, 如果需要限制网络中接

入的用户数量可以打开该功能。如果出现端口无法配置 MAC 地址数量限制功能的情况，请检查交换机的端口是否运行了 **Spanning-tree**, **dot1x**, 端口汇聚或者端口已经配置为 MAC 绑定端口。MAC 数量限制在端口上与这些配置是互斥的，如果该端口要打开 MAC 地址数量限制功能，就必须首先确认端口下的上述功能已经被关闭。

如果在正常配置下，启动了端口、VLAN 中 MAC、IP 数量限制功能后，可以使用 **debug** 各个相关限制的调试命令，查看数量限制的具体信息，以及数量限制功能是否正确，如果有什么问题可以将结果发送给技术服务中心。

第4章 AM功能操作配置

4.1 AM功能简介

AM（Access Management—访问管理）是指当交换机收到 IP 报文或 ARP 报文时，它用收到报文的信息（源 IP 地址或者源 MAC-IP 地址）与配置硬件地址池相比较，如果在配置硬件地址池中找到与收到的报文相匹配的信息（源 IP 地址或者源 MAC-IP 地址）则转发该报文，否则丢弃。之所以在基于源 IP 地址的访问管理上增加基于源 MAC-IP 的访问管理，是因为对主机而言，IP 地址是可变的。如果只有 IP 绑定，用户可以把主机 IP 地址改为转发 IP，从而使本主机发出的报文能够被交换机转发。而 MAC-IP 可以与主机唯一绑定，所以为了防止用户恶意修改主机 IP 地址来使本主机发出的报文能被交换机转发，MAC-IP 的绑定是必要的。

通过 AM 访问管理的端口绑定特性，网络管理员可以将合法用户的 IP（MAC-IP）地址绑定到指定的端口上。进行绑定操作后，只有指定 IP（MAC-IP）地址的用户发出的报文才能通过该端口转发，增强了用户对网络安全的监控。

4.2 AM功能配置任务序列

- 1. 启动 AM 功能
- 2. 启动某端口的 AM 功能
- 3. 配置转发 IP
- 4. 配置转发 MAC-IP
- 5. 删除所有已配置的转发 IP 或 MAC-IP 或全部
- 6. 显示 AM 相关配置信息

1. 启动 AM 功能

命令	解释
全局配置模式	
am enable no am enable	全局启动或关闭 AM 功能。

2. 启动某端口的 AM 功能

命令	解释
端口配置模式	
am port no am port	启动/关闭端口的 AM 功能，端口 AM 功能启动后，默认禁止所有的 IP 报文与 ARP 报文转发。

3. 配置转发 IP

命令	解释
端口配置模式	
am ip-pool <ip-address> <num> no am ip-pool <ip-address> <num>	配置端口的转发 IP。

4. 配置转发 MAC-IP

命令	解释
端口配置模式	
am mac-ip-pool <mac-address> <ip-address> no am mac-ip-pool <mac-address> <ip-address>	配置端口的转发 MAC-IP。

5. 删除所有已配置的转发 IP 或 MAC-IP 或全部

命令	解释
全局配置模式	
no am all [ip-pool mac-ip-pool]	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。

6. 显示 AM 相关配置信息

命令	解释
全局配置模式	
show am [interface <interface-name>]	显示全部或某一特定端口的 AM 配置信息。

4.3 AM功能典型案例

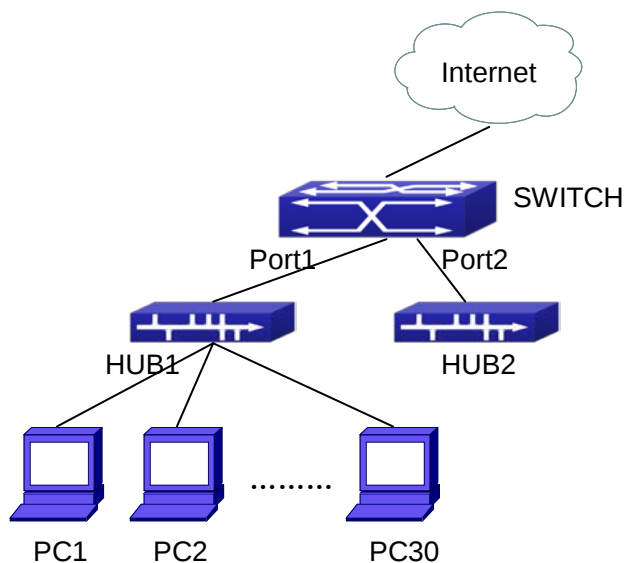


图 4-1 AM 功能典型配置案例

在上述网络拓扑图中，30 台 PC 通过 HUB1 汇集后与交换机的端口 1 相连，30 台 PC 的 IP 地址范围 100.10.10.1~100.10.10.30，出于安全考虑，系统管理员认为只有 IP 地址范围在 100.10.10.1~100.10.10.10 内的用户为合法用户，交换机只能对合法用户发来的数据包进行转发，对 IP 地址不在该范围内的用户发来的数据包，交换机不能转发，直接丢弃。

基于上述要求，在交换机上可做如下配置：

```
Switch(config)#am enable
Switch(config)#interface ethernet1/0/1
Switch(Config-If-Ethernet 1/0/1)#am port
Switch(Config-If-Ethernet 1/0/1)#am ip-pool 10.10.10.1 10
```

4.4 AM功能排错帮助

AM 功能默认是关闭的，打开 AM 功能后，可以进行 AM 的相关配置。

可以使用 `show am` 来查看当前 AM 配置，包括 AM 是否打开，各个端口所配置的 AM 信息等，也可以使用 `show am [interface <interface-name>]` 来查看具体端口的 AM 配置信息。

在操作过程中，如果有操作错误，系统将会给出具体的错误提示信息。

第5章 安全特性配置

5.1 安全特性介绍

在介绍安全特性之前，先介绍一下 DoS 的概念。DoS 是 Denial of Service 的缩写，意为拒绝服务。DoS 攻击是网络上一种简单但很有效的破坏性攻击手段，服务器会由于不停顿地处理攻击者的数据包，从而正常用户发送的数据包会被丢弃，得不到处理，从而造成了服务器的拒绝服务，更严重的会导致服务器敏感数据泄漏。

安全特性是指利用协议检查来防范 DoS 攻击等安全应用，协议检查允许用户基于给定条件丢弃满足条件的报文。安全特性为用户提供了若干种简单有效的防御 DoS 攻击的方法，并且不影响交换机的线性转发性能。

5.2 安全特性配置

5.2.1 防IP Spoofing功能配置任务序列

使能 IP Spoofing 功能

命令	解释
全局配置模式	
[no] dosattack-check srcip-equal-dstip enable	开启(关闭)检查 IP 源地址等于目的地址的功能。

5.2.2 防TCP非法标志攻击功能配置任务序列

1. 使能 TCP 非法标志攻击功能

2. 使能检查 IPv4 分片功能

命令	解释
全局配置模式	
[no] dosattack-check tcp-flags enable	开启(关闭)检查 TCP 标志功能。
[no] dosattack-check ipv4-first-fragment enable	开启(关闭)检查 IPv4 分片功能，单独使用该命令无作用，若不开启该功能，交换机不会丢弃包含了非法 TCP 标志的 IPv4 分片报文。

5.2.3 防端口欺骗功能配置任务序列

1. 使能防端口欺骗功能

命令	解释
全局配置模式	
[no] dosattack-check srcport-equal-dstport enable	开启(关闭)防端口欺骗功能。
[no] dosattack-check ipv4-first-fragment enable	开启(关闭)检查 IPv4 分片功能，单独使用该命令无作用，若不开启该功能，交换机不会丢弃源端口等于目的端口的 IPv4 分片报文。

5.2.4 防TCP碎片攻击功能配置任务序列

1. 使能防 TCP 碎片攻击功能
2. 设置允许通过的最小 TCP 报文段长度

命令	解释
全局配置模式	
[no] dosattack-check tcp-fragment enable	开启(关闭)防 TCP 碎片攻击功能。
dosattack-check tcp-segment <size>	设置允许通过的最小 TCP 报文段长度，单独使用该命令无作用，需要开启 dosattack-check tcp-fragment enable 。

5.2.5 防ICMP碎片攻击功能配置任务序列

1. 使能防 ICMP 碎片攻击功能
2. 设置允许通过的最大的 ICMPv4 净荷长度
3. 设置允许通过的最大的 ICMPv6 净荷长度

命令	解释
全局配置模式	
[no] dosattack-check icmp-attacking enable	开启防(关闭)ICMP 碎片攻击功能。
dosattack-check icmpV4-size <size>	设置允许通过的最大的 ICMPv4 净荷长度，单独使用该命令无作用，需要开启 dosattack-check icmp-attacking enable 。
dosattack-check icmpV6-size <size>	设置允许通过的最大的 ICMPv6 净荷长度，单独使用该命令无作用，需要开启 dosattack-check icmp-attacking enable 。

5.3 安全特性举例

案例：

用户有如下配置需求：交换机不转发源 IP 地址等于目的 IP 地址的数据报，和源端口等于目的端口的数据报，且在 IPv4 网络内只允许使用默认选项的 ping 命令，即 ICMP request 报文不可分片，且净荷长度一般小于 100。

配置步骤如下：

```
Switch(config)#dosattack-check srcip-equal-dstip enable
Switch(config)#dosattack-check srcport-equal-dstport enable
Switch(config)#dosattack-check ipv4-first-fragment enable
Switch(config)#dosattack-check icmp-attacking enable
Switch(config)#dosattack-check icmpV4-size 100
```

第6章 TACACS+配置

6.1 TACACS+简介

TACACS+终端访问控制器访问控制协议是类似于radius协议的一个用于控制终端接入网络的协议。该协议同样提供Authentication(认证), Authorrization(授权), Accounting(记帐)三个独立的功能。与RADIUS 相比, TACACS+采用TCP协议作为传输层, 并且对报文主体(除标准报文头)加密, 因而具有更加可靠的传输和加密特性, 更加适合于安全控制。

根据TACACS+(version 1.78)协议的特点。我们在交换机上提供了TACACS+的认证功能。用户在登录交换机后(例如telnet)可以利用TACACS+来进行用户名和密码的验证。

6.2 TACACS+配置

1. 配置 TACACS+认证密钥
2. 配置 TACACS+服务器
3. 配置 TACACS+认证超时时间
4. 配置 TACACS+ NAS-IP 地址

1. 配置 TACACS+认证密钥

命令	解释
全局配置模式	
tacacs-server key {0 7} <string> no tacacs-server key	设置 TACACS+服务器的密钥; 本命令的 no 操作为删除 TACACS+服务器的密钥。

2. 配置 TACACS+ Server

命令	解释
全局配置模式	
tacacs-server authentication host <ip-address> [port <port-number>] [timeout <seconds>] [key {0 7} <string>] [primary] no tacacs-server authentication host <ip-address>	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。

3. 配置 TACACS+认证超时时间

命令	解释
全局配置模式	

tacacs-server timeout <seconds> no tacacs-server timeout	配置 TACACS+服务器认证超时时间；本命令的 no 操作为恢复缺省配置。
4. 配置 TACACS+ NAS-IP 地址	
命令	解释
全局配置模式	
tacacs-server nas-ipv4 <ip-address> no tacacs-server nas-ipv4	设置交换设备发送 TACACS+报文的 IP 源地址。

6.3 TACACS+典型案例

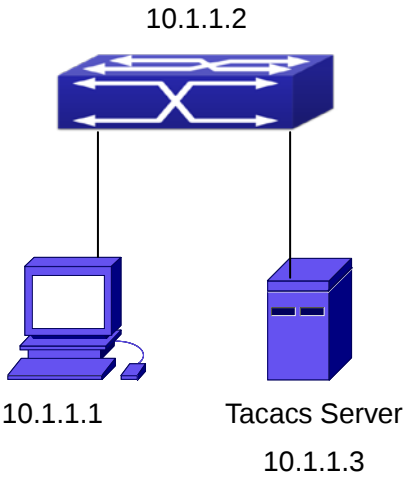


图 6-1 TACACS+配置示意图

计算机连接到交换机，交换机的 IP 地址设置为 10.1.1.2，并与一个 TACACS+认证服务器相连接，TACACS+认证服务器的 IP 地址设置为 10.1.1.3，认证端口为缺省端口 49。交换机的 telnet 登录认证方式设置为 tacacs local。计算机利用 telnet 登录交换机，交换机通过使用 TACACS+认证服务器实现对 telnet 用户的认证。

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#tacacs-server authentication host 10.1.1.3
Switch(config)#tacacs-server key test
Switch(config)#authentication line vty login tacacs
```

6.4 TACACS+排错帮助

在配置、使用 TACACS+协议时，可能会由于物理连接、配置错误等原因导致 TACACS+

认证失败。因此，用户应注意以下要点：

- ☞ 首先应该保证到 TACACS+服务器的物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 `show interface` 命令）；
- ☞ 再次，保证交换机配置的 TACACS+密钥同 TACACS+服务器上配置的密钥一致；
- ☞ 然后，确保配置了正确的 TACACS+服务器。

第7章 RADIUS配置

7.1 RADIUS简介

7.1.1 AAA与RADIUS简介

AAA是Authentication，Authorization and Accounting（认证、授权和计费）的简称，它提供了网络安全管理的一致性框架，该框架通过认证、授权和计费三大功能满足了安全网络的访问控制需求：哪些用户可以访问网络设备，访问用户拥有哪些访问权限以及用户使用网络资源的统计计费。

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的、客户端/服务器结构的信息交互协议。RADIUS客户端一般在网络设备上启用，与802.1x协议结合实现认证、授权和计费的所有主要功能，而RADIUS服务器负责维护用户认证、授权和计费信息数据库，通过RADIUS协议与客户端进行通信，完成用户认证和授权信息的下发以及计费信息的统计。RADIUS协议是实现AAA框架最常用的一种协议。

7.1.2 RADIUS协议的报文结构

RADIUS 协议采用 UDP 报文来承载协议报文，报文格式如下：

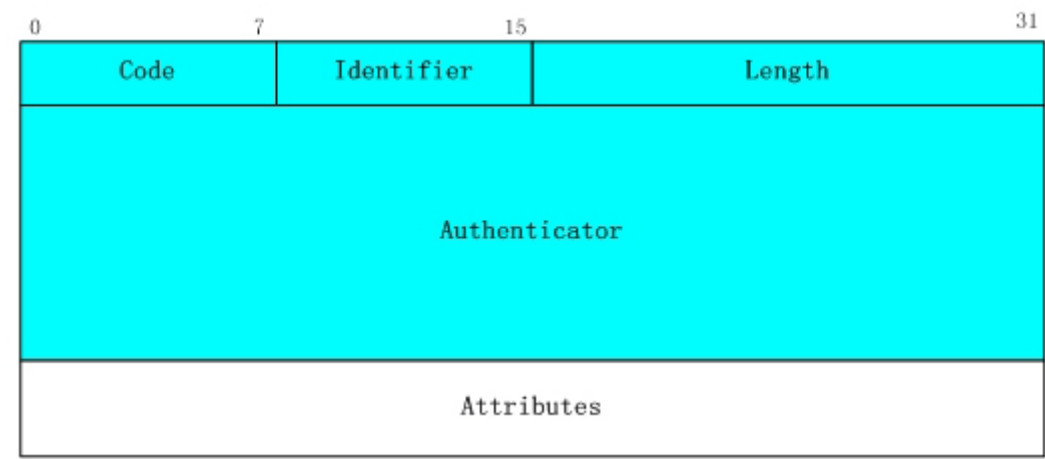


图 7-1 RADIUS 报文结构

Code 域（1 字节）：表示 RADIUS 报文的类型，取值如下，

- 1 Access-Request 认证请求报文
- 2 Access-Accept 认证接收报文
- 3 Access-Reject 认证拒绝报文
- 4 Accounting-Request 计费请求报文
- 5 Accounting-Response 计费回应报文

11 Access-Challenge 认证Challenge报文

Identifier 域（1 字节）：用作报文标识，用于匹配请求与应答报文。

Length 域（2 字节）：表示整个 RADIUS 报文的长度，包括 Code、Identifier、Length、Authenticator 和 Attributes 域。

Authenticator 域（16 字节）：用于验证 RADIUS 服务器回应的报文，还能用于密码隐藏算法。分为 Request Authenticator 和 Response Authenticator。

Attribute 域：用于携带指明的认证和授权以及计费等相关信息，提供请求和相应报文的详细配置信息。Attribute 域采用（Type、Length、Value）三元组的形式构造。

☞ Type 字段（1 字节），表示属性的类型值，如下表列举出常用属性。

属性	属性类型	属性	属性类型
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

- ☞ Length 字段（1 字节），表示属性长度（包括 Type、Length 和 Value 字段），单位为字节。
- ☞ Value 字段，表示属性的具体信息，其格式和内容由类型域和长度域决定。

7.2 RADIUS配置

1. 使能交换机的 AAA 认证和计费功能
2. 配置 RADIUS 认证密钥
3. 配置 RADIUS 服务器
4. 配置 RADIUS 服务的参数
5. 配置 RADIUS NAS-IP 地址

1. 使能交换机的 AAA 认证和计费功能

命令	解释
全局配置模式	
aaa enable no aaa enable	使能交换机的 AAA 认证功能；本命令的 no 操作为关闭交换机的 AAA 认证功能。
aaa-accounting enable no aaa-accounting enable	使能交换机的计费功能；本命令的 no 操作为关闭交换机的计费功能。
aaa-accounting update {enable disable}	打开或关闭计费更新功能。

2. 配置 RADIUS 认证密钥

命令	解释
全局配置模式	
radius-server key {0 7} <string> no radius-server key	设置 RADIUS 服务器的密钥；本命令的 no 操作为删除 RADIUS 服务器的密钥。

3. 配置 RADIUS Server

命令	解释
全局配置模式	

radius-server authentication host {<ipv4-address> <ipv6-address>} [port <port-number>] [key {0 7} <string>] [primary] [access-mode {dot1x telnet wireless}] no radius-server authentication host {<ipv4-address> <ipv6-address>}	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。
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>}	配置 RADIUS 计费服务器的 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。

4. 配置 RADIUS 服务参数

命令	解释
全局配置模式	
radius-server dead-time <minutes> no radius-server dead-time	配置 RADIUS 服务器 down 机后的恢复时间；本命令的 no 操作为恢复缺省配置。
radius-server retransmit <retries> no radius-server retransmit	配置 RADIUS 重传次数；本命令的 no 操作为恢复缺省配置。
radius-server timeout <seconds> no radius-server timeout	配置 RADIUS 服务器的超时定时器；本命令的 no 操作为恢复缺省配置。
radius-server accounting-interim-update timeout <seconds> no radius-server accounting-interim-update timeout	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。

5. 配置 RADIUS NAS-IP 地址

命令	解释
全局配置模式	
radius nas-ipv4 <ip-address> no radius nas-ipv4	设置交换设备发送 RADIUS 报文的 IP 源地址。
radius nas-ipv6 <ipv6-address> no radius nas-ipv6	设置交换设备发送 RADIUS 报文的 IPv6 源地址。

7.3 RADIUS 典型案例

7.3.1 IPv4 Radius 应用举例

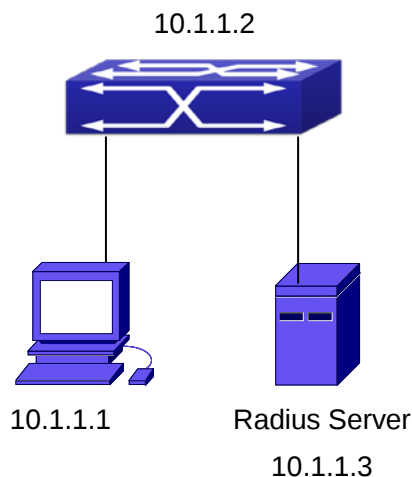


图 7-2 IEEE802.1x 配置举例拓扑图

交换机的 IP 地址设置为 10.1.1.2，并将除端口 Ethernet1/0/2 以外的任意一个端口与 RADIUS 认证服务器相连接，RADIUS 认证服务器的 IP 地址设置为 10.1.1.3，认证、计费端口为缺省端口 1812 和端口 1813。

配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

7.3.2 IPv6 Radius 应用举例

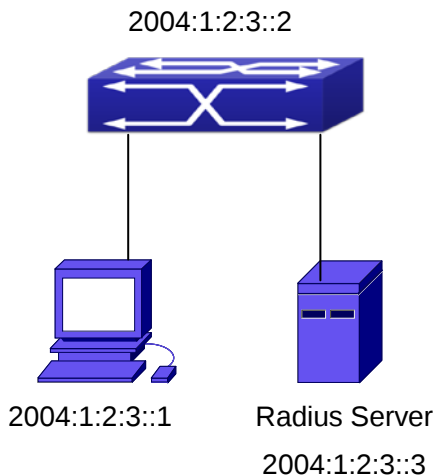


图 7-3 IPv6 Radius 配置举例拓扑图

交换机的 IP 地址设置为 2004:1:2:3::2，并将除端口 1/0/2 以外的任意一个端口与 RADIUS 认证服务器相连接，RADIUS 认证服务器的 IP 地址设置为 2004:1:2:3::3，认证、计费端口为缺省端口 1812 和端口 1813。

配置步骤如下：

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

7.4 RADIUS排错帮助

在配置、使用 RADIUS 协议时，可能会由于物理连接、配置错误等原因导致 RADIUS 认证失败。因此，用户应注意以下要点：

- ☞ 首先应该保证到 RADIUS 服务器的物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 再次，保证交换机配置的 RADIUS 密钥同 RADIUS 服务器上配置的密钥一致；
- ☞ 然后，确保配置了正确的 RADIUS 服务器。

如果使用检查都尝试仍无法解决 RADIUS 认证的问题，那么请使用 debug aaa 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

第8章 SSL配置

8.1 SSL简介

随着计算机网络技术向整个经济社会各层次延伸，整个社会表现对 Internet、Intranet、Extranet 等使用的更大的依赖性。随着企业间信息交互的不断增加，任何一种网络应用和增值服务的使用程度将取决于所使用网络的信息安全有无保障，网络安全已成为现代计算机网络应用的最大障碍，也是急需解决的难题之一。

由于 Web 上有时要传输重要或敏感的数据，因此 Netscape 公司在推出 Web 浏览器首版的同时，提出了安全通信协议 SSL (Secure Socket Layer)，目前已有 2.0 和 3.0 版本。2.0 版本存在安全漏洞，现在已经不使用了，我们的交换机也不支持该版本。SSL 采用公开密钥技术。其目标是保证两个应用间通信的保密性和可靠性，可在服务器和客户机两端同时实现支持。目前，利用公开密钥技术的 SSL 协议，并已成为 Internet 上保密通讯的工业标准。现行 Web 浏览器普遍将 HTTP 和 SSL 相结合，从而实现安全通信。

安全通信协议(SSL)是在 Internet 基础上提供的一种保证私密性的安全协议。它能使客户/服务器应用之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户进行认证。SSL 协议要求建立在可靠的传输层协议(例如：TCP)之上。SSL 协议的优势在于它是与应用层协议独立无关的。高层的应用层协议(例如：HTTP, FTP, TELNET.....)能透明的建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。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。

通过以上叙述，SSL 协议提供的安全信道有以下三个特性：

- ☞ 私密性。因为在握手协议定义了会话密钥后，所有的消息都被加密。
- ☞ 确认性。因为尽管会话的客户端认证是可选的，但是服务器端始终是被认证的。
- ☞ 可靠性。因为传送的消息包括消息完整性检查(使用MAC)。

8.1.1 SSL基本原理

SSL 采用的基本的策略在两个通信程序之间提供一条在其间传递任意应用数据的安全通道。从理论上讲，SSL 连接非常类似“保密的”TCP 连接。协议栈中的 SSL 位置正好位于应用层的下面，TCP 的上面。SSL 假定其下层的数据包发送机制是可靠的。写入网络的数据将依顺序发送给另一端的程序，不会出现丢包或重复发送的情况。从理论上讲，有许多传输协议都能提供此种服务，但在实际应用中，SSL 几乎只是在 TCP 上运行，它不能在 UDP 或直接在 IP 上运行。

当在交换机上运行 web 功能时，当客户端通过浏览器访问我们的 Web 时，我们可以使能 SSL 功能，客户和交换机之间的通信通过 SSL 连接进行，这样很好地提高了访问的安全性。

首先我们在交换机上启动 SSL 功能，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。

使用 SSL 的时，首先进行 SSL 握手的过程，服务器端必须提供证书功能，目前我们使用的证书不是权威机构颁发的正规证书，而是 linux 下自己生成的证书，可能浏览器不能识别。考虑到我们使用 SSL 的环境，使用正规的证书没有必要，我们只要保证用户和交换机之间安全进行通信就可以了。目前我们不要求客户端证书验证功能。在握手的过程中还要协商通信中使用的密钥和加密算法，在交换应用数据的时候使用。

SSL 握手的基本过程：



8.2 SSL配置任务序列

- 1. 启动/关闭 SSL 功能
- 2. 配置/删除 SSL 使用的端口号
- 3. 配置/删除 SSL 使用的加密套件
- 4. SSL 功能的维护与诊断

1. 启动/关闭 SSL 功能

命令	解释
全局配置模式	
ip http secure-server no ip http secure-server	启动/关闭 SSL 功能。

2. 配置/删除 SSL 使用的端口号

命令	解释
全局配置模式	
ip http secure-port <port-number> no ip http secure-port	配置 SSL 使用的端口号，no 命令删除 SSL 使用的端口号。

3. 配置/删除 SSL 加密套件

命令	解释
全局配置模式	
ip http secure-ciphersuite {des-cbc3-sha rc4-128-sha des-cbc-sha} no ip http secure-ciphersuite	配置/删除 SSL 使用的加密套件。

4. SSL 功能的维护与诊断

命令	解释
特权模式或者配置模式	
show ip http secure-server status	显示配置的 SSL 信息。
debug ssl no debug ssl	打开/关闭 SSL 功能的 DEBUG 显示。

8.3 SSL典型案例

当在交换机上运行 web 功能时，当客户端通过浏览器访问我们的 Web 时，我们可以使用 SSL 功能，客户和交换机之间的通信通过 SSL 连接进行，这样很好地提高了访问的安全性。

首先我们在交换机上启动 SSL 功能，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。

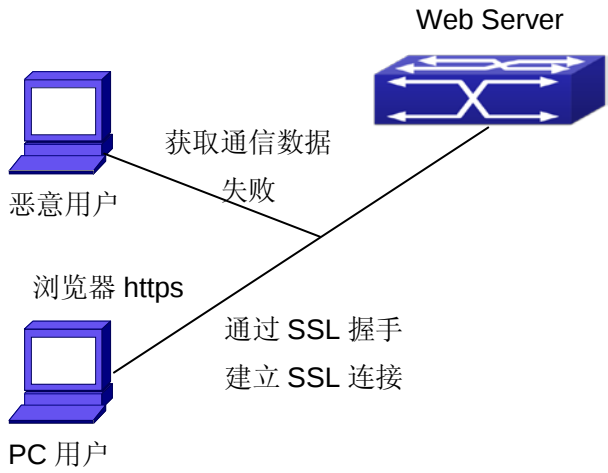


图 8-1 SSL 案例示意图

我们在交换机上进行如下配置：

```
Switch(config)#ip http secure-server
```

```
Switch(config)#ip http secure-port 1025
```

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

8.4 SSL排错帮助

在配置、使用 SSL 功能时，可能会由于物理连接、配置错误等原因导致 SSL 功能异常。

因此，用户应注意以下要点：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，保证接口和链路协议是 UP（使用 show interface 命令）；
- ☞ 然后，确保开启了 SSL 功能(使用 ip http secure-server 命令)；
- ☞ 如果配置了端口，不使用默认的端口号，注意输入网址的时候指明端口号；
- ☞ 如果先启动了 SSL 功能,再进行配置、取消端口号和加密套件操作时需要等到重启 SSL 功能后才生效；
- ☞ 使用 des-cbc-sha 加密套件时，必须 ie7.0 以上的浏览器才能支持；
- ☞ 如果尝试使用以上检查仍无法解决 SSL 的问题，那么请使用 debug ssl 等调试命令，然后将 3 分钟内的 DEBUG 信息拷贝下来，发送给本公司技术服务中心。

第9章 IPv6 安全RA配置

说明：
本章所指的路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

9.1 IPv6 安全RA简介

在 IPv6 网络中，一般的网络拓补结构是由路由器、二层交换机、IPv6 主机构成。通常路由器公告 RA，包括链路前缀、链路 MTU 等信息，IPv6 主机收到 RA 后，生成链路地址，并将默认路由指向发送 RA 的路由器，从而可以进行 IPv6 网络通信。如果恶意的 IPv6 主机发送 RA，使正常的 IPv6 用户将默认路由指向恶意的 IPv6 主机用户，那么就可截获别的用户信息，影响网络安全。同时正常的用户获得另外的地址，使自己无法链接网络。所以我们要实现安全 RA 功能，在交换机的端口通过命令配置拒绝接收恶意的 RA 报文，这样在一定程度上防止恶意 RA 的转发，可以避免影响网络的正常工作。

9.2 IPv6 安全RA配置任务序列

- 1. 全局启动 IPv6 安全 RA
- 2. 端口启动 IPv6 安全 RA
- 3. 显示和调试 IPv6 安全 RA 相关信息

1. 全局启动 IPv6 安全 RA

命令	解释
全局配置模式	
ipv6 security-ra enable no ipv6 security-ra enable	全局模式启动和关闭 IPv6 安全 RA。

2. 端口启动 IPv6 安全 RA

命令	解释
端口配置模式	
ipv6 security-ra enable no ipv6 security-ra enable	端口模式启动和关闭 IPv6 安全 RA。

3. 显示和调试 IPv6 安全 RA 相关信息

命令	解释
特权配置模式	
debug ipv6 security-ra no debug ipv6 security-ra	打开 IPv6 安全 RA 模块的调试信息，本命令的 NO 操作关闭 IPv6 安全 RA 调试信息输出。

<code>show ipv6 security-ra [interface <interface-list>]</code>	显示非信任端口和全局安全 RA 是否启动。
---	-----------------------

9.3 IPv6 安全RA典型案例

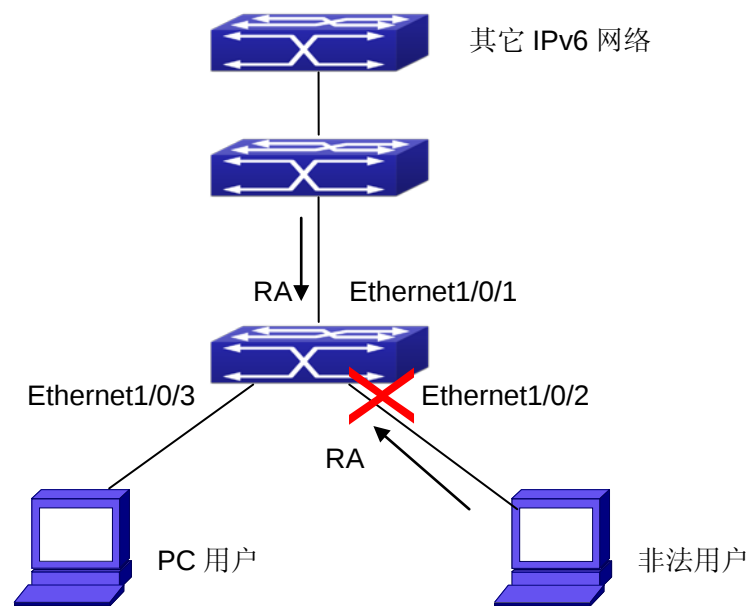


图 9-1 IPv6 安全 RA 案例示意图

说明：图中如果非法用户公告 RA，正常的 PC 用户将收到 RA，将默认路由指向恶意的 IPv6 主机用户，并改变自己的地址，自己将无法链接网络。我们要在交换机的 1/0/2 端口设置安全 RA，那么非法用户的 RA 报文将不会影响到正常的用户。

SWITCH 配置任务序列：

```
Switch#config
Switch(config)#ipv6 security-ra enable
Switch(Config-If-Ethernet1/0/2)#ipv6 security-ra enable
```

9.4 IPv6 安全RA排错帮助

- IPv6 安全 RA 的功能非常简单，如果在配置 IPv6 安全 RA 后，发现功能与预期不符：
- ☞ 判断是否因为交换机是否正确配置。
 - ☞ 判断是否因为交换机配置了与安全 RA 功能冲突的规则使 RA 报文转发。

第10章 VLAN-ACL配置

10.1 VLAN-ACL功能简介

用户通过对 VLAN 配置 ACL 策略，从而实现对 VLAN 内所有端口的访问控制，VLAN-ACL 使用户能够更加方便地管理网络。用户只需在 VLAN 下配置 ACL 策略，相应的 ACL 动作就能在 VLAN 的所有成员端口生效，而无需在每个成员端口上单独配置。

当 VLAN ACL 与 Port ACL 同时配置时，即需要满足 deny 优先，当报文同时匹配 VLAN ACL 和端口 ACL 时，只要有一个动作是 drop，则结果就是 drop。

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 VLAN 入口方向上可以同时配置四种 ACL；在 VLAN 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 VLAN 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 VLAN 上只能配置一条。

10.2 VLAN-ACL功能配置任务序列

- 1. 配置 IP 类型的 VLAN-ACL
- 2. 配置 MAC 类型的 VLAN-ACL
- 3. 配置 MAC-IP 类型的 VLAN-ACL
- 4. 配置 IPv6 类型的 VLAN-ACL
- 5. 显示 VLAN-ACL 的配置及统计信息
- 6. 清除 VLAN-ACL 的统计信息

1. 配置 IP 类型的 VLAN-ACL

命令	解释
全局配置模式	
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	配置或删除 IP 类型的 VLAN-ACL。

2. 配置 MAC 类型的 VLAN-ACL

命令	解释
----	----

全局配置模式	
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	配置或删除 MAC 类型的 VLAN-ACL。

3. 配置 MAC-IP 类型的 VLAN-ACL

命令	解释
全局配置模式	
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	配置或删除 MAC-IP 类型的 VLAN-ACL。

4. 配置 IPv6 类型的 VLAN-ACL

命令	解释
全局配置模式	
vacl ipv6 access-group (<500-699> WORD) {in out} (traffic-statistic) vlan WORD no ipv6 access-group {<500-699> WORD} {in out} vlan WORD	配置或删除 IPv6 类型的 VLAN-ACL。

5. 显示 VLAN-ACL 的配置及统计信息

命令	解释
特权配置模式	
show vACL [in out] vlan [<vlan-id>]	显示 VACL 的配置及统计信息。

6. 清除 VLAN-ACL 的统计信息

命令	解释
特权配置模式	
clear vACL [in out] statistic vlan [<vlan-id>]	清除 VACL 的统计信息。

10.3 VLAN-ACL功能配置案例

某公司的网络配置如下，将不同部分划分到不同 VLAN，技术部为 Vlan1、财务部为 Vlan2，技术部门要求在每天的休息时间可以访问外网，而财务部出于安全性的考虑在任何时间段均不允许访问外部网络。则可以配置如下策略：

- ☞ 为技术部定制 ACL 策略 VACL_A，在休息时间可以访问外网，规则为 Permit，其他时间段均为 Deny，并应用策略到 Vlan1 上。
- ☞ 为财务部定制 ACL 策略 VACL_B，在任何时间均不允许访问外网，但可以不受限制的访问内网资源，并应用策略到 Vlan2 上。

组网环境如下：

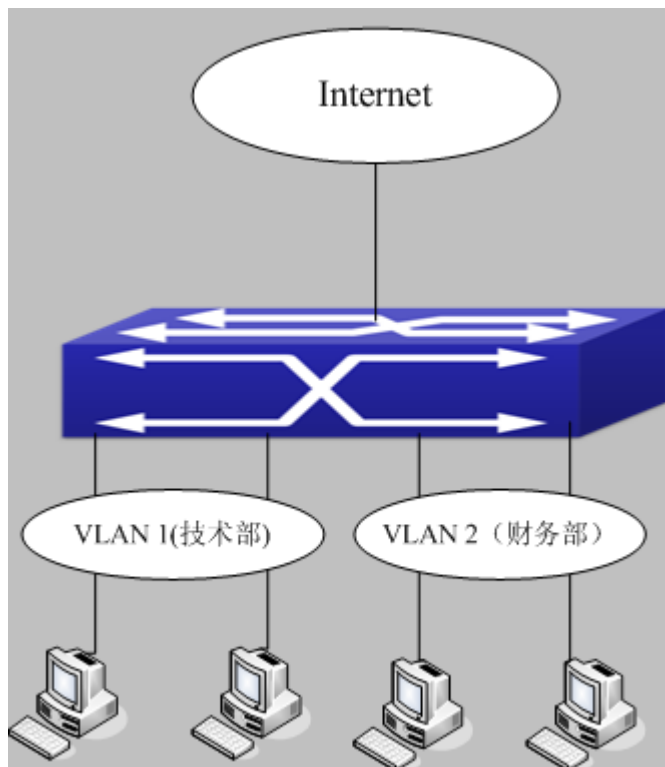


图 10-1 VLAN-ACL 配置案例

配置举例：

- 1) 先配置一个 timerange，有效时间为工作日的上班时间。

```
Switch(config)#time-range t1
```

```
Switch(config-time-range-t1)#periodic weekdays 9:00:00 to 12:00:00
```

```
Switch(config-time-range-t1)#periodic weekdays 13:00:00 to 18:00:00
```

- 2) 配置 IP 的扩展 acl_a，上班时间仅允许访问同一网段（如 192.168.0.255）内的主机。

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

```
Switch(config-ip-ext-nacl-vACL_a)# permit ip any-source 192.168.0.0 0.0.0.255 time-range  
t1
```

```
Switch(config-ip-ext-nacl-vacl_a)# deny ip any-source any-destination time-range t1
```

3) 配置 IP 的扩展 acl_b, 任何时间仅允许访问同一网段 (如 192.168.1.255) 内的主机。

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

```
Switch(config-ip-ext-nacl-vacl_a)# permit ip any-source 192.168.1.0 0.0.0.255
```

```
Switch(config-ip-ext-nacl-vacl_a)# deny ip any-source any-destination
```

4) 将配置应用到 VLAN。

```
Switch(config)#vacl ip access-group vacl_a in vlan 1
```

```
Switch(config)#vacl ip access-group vacl_b in vlan 2
```

10.4 VLAN-ACL排错帮助

- ☞ 当 VLAN ACL 与 Port ACL 同时配置时, 即需要满足 deny 优先, 当报文同时匹配 VLAN ACL 和端口 ACL 时, 只要有一个动作是 drop, 则结果就是 drop。
- ☞ 每一个不同类型的 ACL 在一个 VLAN 上仅能配置一个, 如: 基本的 IP ACL, 在每个 VLAN 上仅能够应用一个。

第11章 MAB配置

说明：
本章所指的三层交换机代表了一般意义下的路由器或运行了路由协议的无线控制产品。

11.1 MAB介绍

在实际网络中存在的无法安装认证客户端的设备，比如打印机、PDA 设备等，由于它们无法安装客户端，所以无法进行 802.1x 认证。但它们又要访问网络中的资源，因此需要使用 MAB 认证，作为对 802.1x 认证的一个重要补充。

MAB 认证是一种基于 MAB 用户接入端口和 MAC 地址的网络接入认证方式，MAB 用户不需要安装任何认证客户端，认证设备在收到 MAB 用户发出的 ARP 报文后，根据 MAB 用户 MAC 地址发起认证，认证服务器存有 MAB 用户 MAC 对应的认证信息。认证通过后，放行匹配端口和源 MAC 的报文。认证过程中，不需要 MAB 用户手动输入认证用户名和密码。

目前 MAB 认证设备只支持 RADIUS 认证方式，认证设备对于认证用户名和密码选择的方式如下：使用 MAB 用户的 MAC 地址作为认证的用户名和密码，或者固定用户名和密码（即不论用户的 MAC 地址为何值，所有用户均使用在设备上预先配置的用户名和密码进行认证）。

11.2 MAB基本配置

MAB 配置任务序列如下：

- 1. 开启 MAB 功能
 - 1) 开启全局的 MAB 功能
 - 2) 开启端口的 MAB 功能
- 2. 配置 MAB 认证用户名及密码
- 3. 配置 MAB 参数
 - 1) 配置 MAB 认证的 guest-vlan
 - 2) 配置 MAB 认证的端口绑定数目
 - 3) 配置 MAB 认证的重认证时间
 - 4) 配置 MAB 认证的下线检测时间
 - 5) 配置 MAB 认证的其他参数

- 1. 开启 MAB 功能

命令	解释
全局配置模式	

mac-authentication-bypass enable no mac-authentication-bypass enable	打开 MAB 认证功能全局开关。
端口配置模式	
mac-authentication-bypass enable no mac-authentication-bypass enable	打开 MAB 认证功能端口开关。

2. 配置 MAB 认证用户名及密码

命令	解释
全局配置模式	
mac-authentication-bypass username-format {mac-address {fixed username WORD password WORD}}	设置 MAB 认证功能的认证方式。

3. 配置 MAB 参数

命令	解释
端口配置模式	
mac-authentication-bypass guest-vlan <1-4094> no mac-authentication-bypass guest-vlan	设置 MAB 认证的 guest vlan，此命令只能在 hybrid 端口上使用，在 access 端口上使用无效。
mac-authentication-bypass binding-limit <1-100> no mac-authentication-bypass binding-limit	设置端口上允许建立的最大 MAB 绑定数目。
全局配置模式	
mac-authentication-bypass timeout reauth-period <1-3600> no mac-authentication-bypass timeout reauth-period	设置认证失败后，重新尝试认证的时间间隔。
mac-authentication-bypass timeout offline-detect (0 <60-7200>) no mac-authentication-bypass timeout offline-detect	设置下线检测时间间隔。
mac-authentication-bypass timeout quiet-period <1-60> no mac-authentication-bypass timeout quiet-period	设置 MAB 认证的静默时间。

mac-authentication-bypass timeout stale-period <0-60> no mac-authentication-bypass timeout stale-period	设置端口 down 后，延时删除绑定的时间。
mac-authentication-bypass timeout linkup-period <0-30> no mac-authentication-bypass timeout linkup-period	设置 MAB 绑定转变 vlan 时，为了重新获取 IP，down/up 的时间间隔。
authentication mab {radius local} (none) no authentication mab	配置 MAC 地址认证对登录用户的验证方式和验证选择优先级；该命令的 no 命令恢复缺省验证方式。

11.3 MAB 举例

案例：

MAB 认证功能典型应用场景如下图所示：

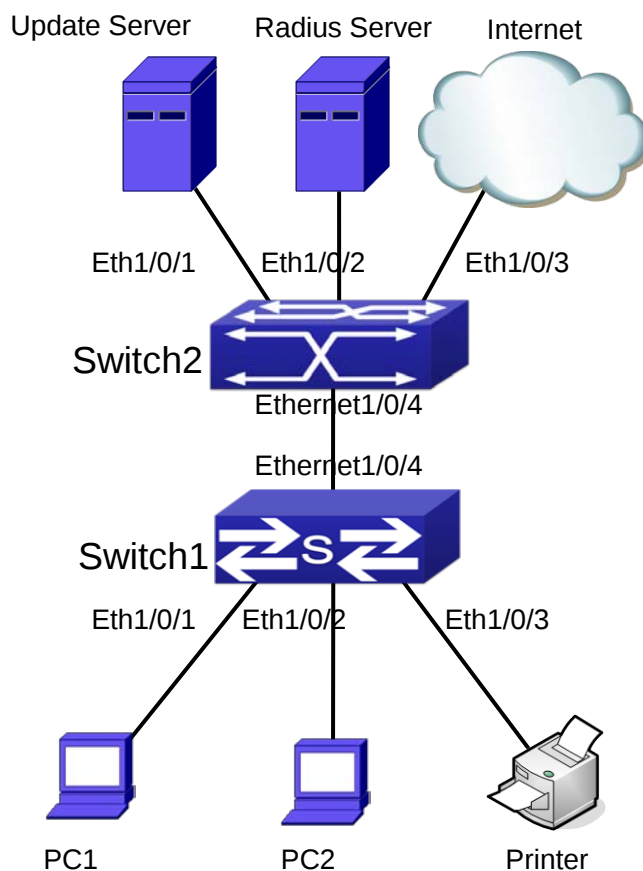


图 11-1 MAB 应用

Switch1 是一个二层的接入交换机，Switch2 是一个三层的汇聚交换机。

交换机 Switch1 中 Ethernet 1/0/1 是 access 端口，连接 PC1,端口打开了 802.1x port-based 功能，并在端口上配置了 guest vlan 为 vlan 8。

Ethernet 1/0/2 是 Hybrid 端口，连接的是 PC2，端口的 native vlan 为 vlan1，并在端口上配置了 guest vlan 为 vlan 8，端口以 untag 的方式加入 vlan1、vlan 8 和 vlan10，端口打开了 MAB 功能。

Ethernet 1/0/3 是 access 端口，连接的是打印机 printer，端口打开了 MAB 功能。

Ethernet 1/0/4 是 trunk 端口，连接三层交换机 Switch2。

交换机 Switch2 中 Ethernet 1/0/4 是 trunk 端口，连接二层交换机 Switch1。

Ethernet 1/0/1 是 access 端口，属于 vlan 8,连接的是一台更新服务器，用于客户端软件的下载和升级。

Ethernet 1/0/2 是 access 端口，属于 vlan 9，连接的是 radius 认证服务器，radius 认证服务器上配置了 auto vlan 为 vlan 10。

Ethernet 1/0/3 是 access 端口，属于 vlan 10，连接的是外部的 internet 资源。

为实现此应用，需按以下方式进行配置：

Switch1 的配置

(1)全局打开 802.1x 和 MAB 认证功能，配置 MAB 认证使用的用户名密码;配置 radius-server 的地址;

```
Switch(config)# dot1x enable
Switch(config)# mac-authentication-bypass enable
Switch(config)#mac-authentication-bypass username-format fixed username
mabuser password mabpwd
Switch(config)#vlan 8-10
Switch(config)#interface vlan 9
Switch(config-if-vlan9)ip address 192.168.61.9 255.255.255.0
Switch(config-if-vlan9)exit
Switch(config)#radius-server authentication host 192.168.61.10
Switch(config)#radius-server accounting host 192.168.61.10
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

(2)打开各个端口的认证功能

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#dot1x enable
Switch(config-if-ethernet1/0/1)#dot1x port-method portbased
Switch(config-if-ethernet1/0/1)#dot1x guest-vlan 8
Switch(config-if-ethernet1/0/1)#exit
```

```
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#switchport mode hybrid
Switch(config-if-ethernet1/0/2)#switchport hybrid native vlan 1
Switch(config-if-ethernet1/0/2)#switchport hybrid allowed vlan 1;8;10 untag
Switch(config-if-ethernet1/0/2)#mac-authentication-bypass enable
Switch(config-if-ethernet1/0/2)#mac-authentication-bypass enable guest-vlan 8
Switch(config-if-ethernet1/0/2)#exit
```

```
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#switchport mode access
Switch(config-if-ethernet1/0/3)#mac-authentication-bypass enable
Switch(config-if-ethernet1/0/3)#exit
```

```
Switch(config)#interface ethernet 1/0/4
```

```
Switch(config-if-ethernet1/0/4)#switchport mode trunk
```

11.4 MAB排错帮助

当在使用 MAB 过程中遇到问题，请检查是否是如下原因：

- ✎ 请确保交换机全局与端口已经打开 MAB 功能。
- ✎ 请确保交换机配置的 MAB 认证使用的用户名与密码正确。
- ✎ 请确保交换机的 radius-server 配置正确。MAB 下线检测是通过查询动态 MAC 是否存在来完成的。如果绑定中的 MAC 地址存在于 MAC 地址表中则维持绑定，如果没有就删除绑定。这样，实际对于用户的无流量下线时间为 1-2 个 MAC 老化周期加上 0-1 个 MAB 下线检测时间。