

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	1-18
1.4 ACL 排错帮助	1-22
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
2.1.5 802.1x 认证方式	2-5
2.1.6 802.1x 的扩展和优化	2-10
2.1.7 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
2.4 802.1x 排错帮助	2-19
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 TACACS+配置.....	5-1
5.1 TACACS+简介.....	5-1
5.2 TACACS+配置.....	5-1
5.3 TACACS+典型案例.....	5-2
5.4 TACACS+排错帮助.....	5-2
第 6 章 RADIUS 配置.....	6-1
6.1 RADIUS 简介.....	6-1
6.1.1 AAA 与 RADIUS 简介.....	6-1
6.1.2 RADIUS 协议的报文结构.....	6-1
6.2 RADIUS 配置.....	6-3
6.3 RADIUS 典型案例.....	6-5
6.3.1 IPv4 Radius 应用举例.....	6-5
6.3.2 IPv6 Radius 应用举例.....	6-5
6.4 RADIUS 排错帮助.....	6-6
第 7 章 SSL 配置.....	7-1
7.1 SSL 简介.....	7-1
7.1.1 SSL 基本原理.....	7-1
7.2 SSL 配置任务序列.....	7-2
7.3 SSL 典型案例.....	7-3
7.4 SSL 排错帮助.....	7-4
第 8 章 IPv6 安全 RA 配置.....	8-1
8.1 IPv6 安全 RA 简介.....	8-1
8.2 IPv6 安全 RA 配置任务序列.....	8-1
8.3 IPv6 安全 RA 典型案例.....	8-2
8.4 IPv6 安全 RA 排错帮助.....	8-2

第 9 章 VLAN-ACL 配置	9-1
9.1 VLAN-ACL 功能简介.....	9-1
9.2 VLAN-ACL 功能配置任务序列.....	9-1
9.3 VLAN-ACL 功能配置案例.....	9-3
9.4 VLAN-ACL 排错帮助.....	9-4
第 10 章 MAB 配置	10-1
10.1 MAB 介绍.....	10-1
10.2 MAB 基本配置.....	10-1
10.3 MAB 举例.....	10-3
10.4 MAB 排错帮助.....	10-5
第 11 章 PPPoE 中间代理配置	11-1
11.1 PPPoE Intermediate Agent 介绍.....	11-1
11.1.1 PPPoE 简介.....	11-1
11.1.2 PPPoE IA 介绍.....	11-1
11.2 PPPoE Intermediate Agent 配置任务序列.....	11-5
11.3 PPPoE Intermediate Agent 典型应用.....	11-7
11.4 PPPoE Intermediate Agent 排错帮助.....	11-8
第 12 章 SAVI 配置	12-1
12.1 SAVI 介绍.....	12-1
12.2 SAVI 配置.....	12-1
12.3 SAVI 典型应用.....	12-4
12.4 SAVI 排错帮助.....	12-6
第 13 章 Captive Portal 认证	13-1
13.1 Captive Portal 认证配置.....	13-1
13.1.1 Captive Portal 认证介绍.....	13-1
13.1.2 Captive Portal 认证配置.....	13-1
13.1.3 Captive Portal 认证举例.....	13-4
13.1.4 Captive Portal 认证排错帮助.....	13-5
13.2 计费功能配置.....	13-6
13.2.1 计费功能介绍.....	13-6

13.2.2 计费功能配置.....	13-6
13.2.3 计费功能举例.....	13-7
13.2.4 计费功能排错帮助.....	13-8
13.3 Free-resource 功能配置.....	13-8
13.3.1 Free-resource 功能介绍.....	13-8
13.3.2 Free-resource 功能配置.....	13-8
13.3.3 Free-resource 功能举例.....	13-8
13.3.4 Free-resource 功能排错帮助.....	13-9
13.4 认证白名单功能配置.....	13-9
13.4.1 认证白名单功能介绍.....	13-9
13.4.2 认证白名单功能配置.....	13-9
13.4.3 认证白名单功能举例.....	13-10
13.4.4 认证白名单功能排错帮助.....	13-10
13.5 认证成功后页面自动推送（暂不支持）.....	13-10
13.5.1 认证成功后页面自动推送介绍.....	13-10
13.5.2 认证成功后页面自动推送配置.....	13-11
13.5.3 认证成功后页面自动推送举例.....	13-11
13.5.4 认证成功后页面自动推送排错帮助.....	13-12
13.6 http-redirect-filter.....	13-13
13.6.1 http-redirect-filter 介绍.....	13-13
13.6.2 http-redirect-filter 配置.....	13-13
13.6.3 http-redirect-filter 举例.....	13-13
13.6.4 http-redirect-filter 排错帮助.....	13-15
13.7 Portal 无感知.....	13-15
13.7.1 Portal 无感知介绍.....	13-15
13.7.2 Portal 无感知配置.....	13-16
13.7.3 Portal 无感知举例.....	13-16
13.7.4 Portal 无感知排错帮助.....	13-17
13.8 Portal 逃生.....	13-18
13.8.1 Portal Server 逃生功能.....	13-18
13.8.2 Radius Server 逃生功能.....	13-21

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) 配置默认动作(default action)

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。
<pre>no access-list <num></pre>	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)

[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>]]]	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	
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>]	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。
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>]	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} {{<slIPv6Prefix/sPrefixlen>} any-source {host-source <slIPv6Addr>}}	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 {{<slIPv6Prefix/sPrefixlen>} any-source {host-source <slIPv6Addr>}} {<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 {<slIPv6Prefix/sPrefixlen> any-source {host-source <slIPv6Addr>}} [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>]	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 {<slIPv6Prefix/sPrefixlen> any-source {host-source <slIPv6Addr>}} [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>]	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> {<slIPv6Prefix/sPrefixlen> any-source {host-source <slIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> any-destination {host-destination <dIPv6Addr>}} [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} {<slIPv6Prefix/sPrefixlen> any-source {host-source <slIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> any-destination {host-destination <dIPv6Addr>}} [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。

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

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

(3) 配置绝对性时段

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

4. 将 accessl-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	
{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}	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	
clear access-group (in out) statistic interface { <interface-name> ethernet <interface-name> }	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：

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

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

```
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.
```

```
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)#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.
```

```
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：

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)#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)#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.
```

```
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)#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.
```

```
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。
- ☞ 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。

第2章 802.1x 配置

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）。

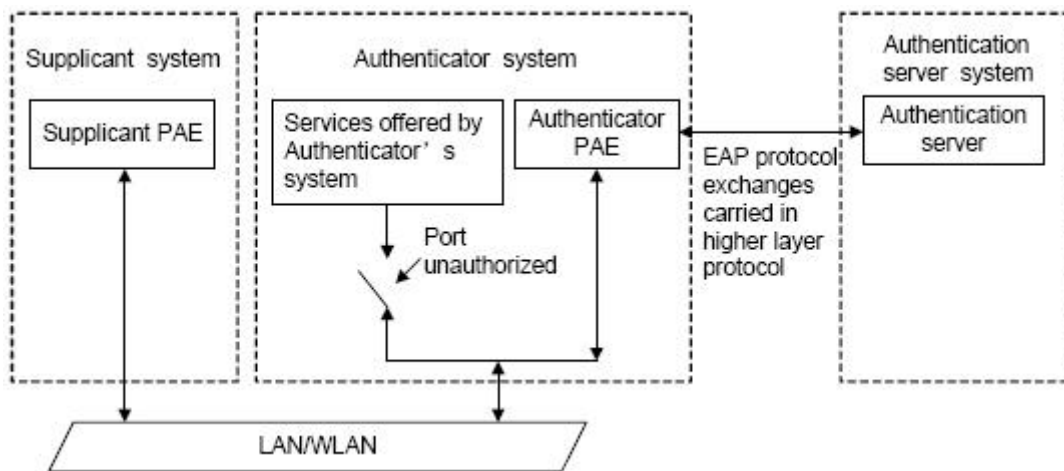


图 2-1 802.1x 认证体系结构

- 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。

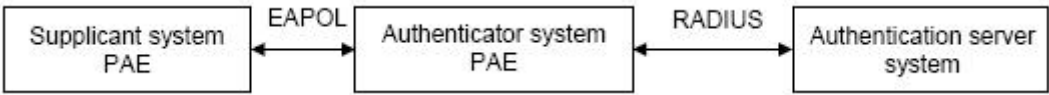


图 2-2 802.1x 认证工作机制

- 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。

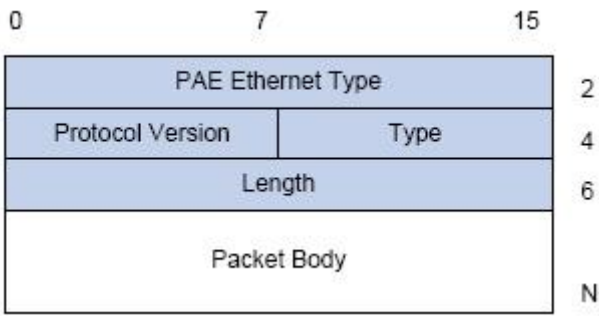


图 2-3 EAPOL 数据包格式

- 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。

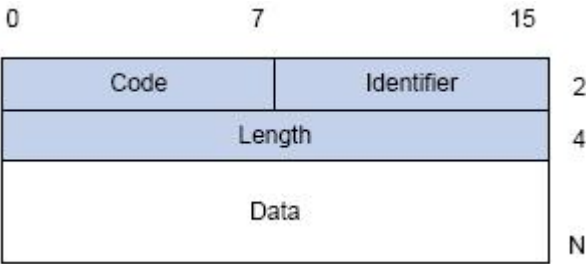


图 2-4 EAP 数据包格式

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。

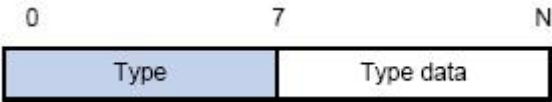


图 2-5 Request 和 Response 类型数据包的 Data 域的格式

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。

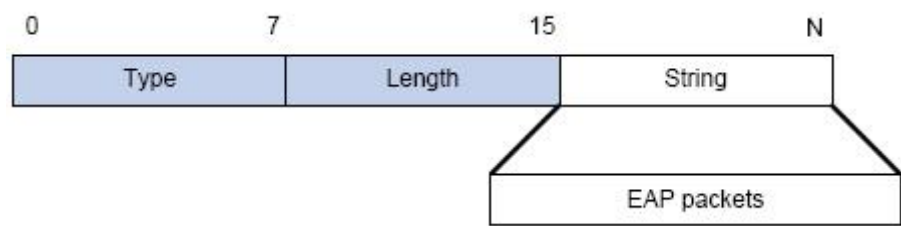


图 2-6 EAP-Message 属性封装

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。

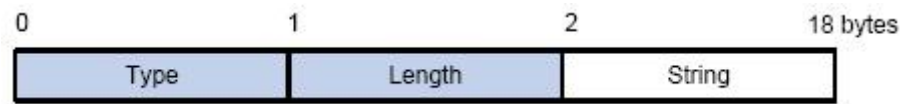


图 2-7 Message-Authenticator 属性

2.1.5 802.1x 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。

2.1.5.1 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。

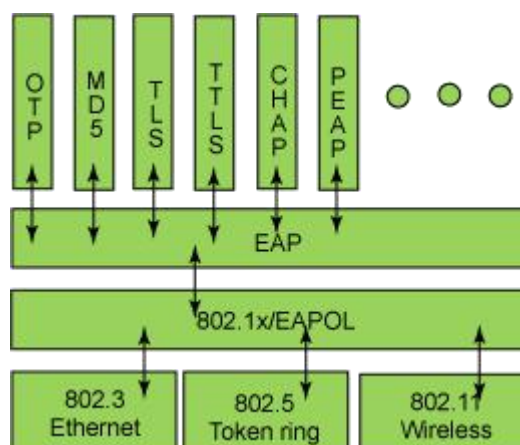


图 2-8 EAP 认证方法协议栈

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：

- 2、**EAP-MD5**
- 3、**EAP-TLS**（Transport Layer Security，传输层安全）
- 4、**EAP-TTLS**（Tunneled Transport Layer Security，隧道传输层安全）
- 5、**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：

- 1、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。
- 2、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，但提供最少的安全，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。

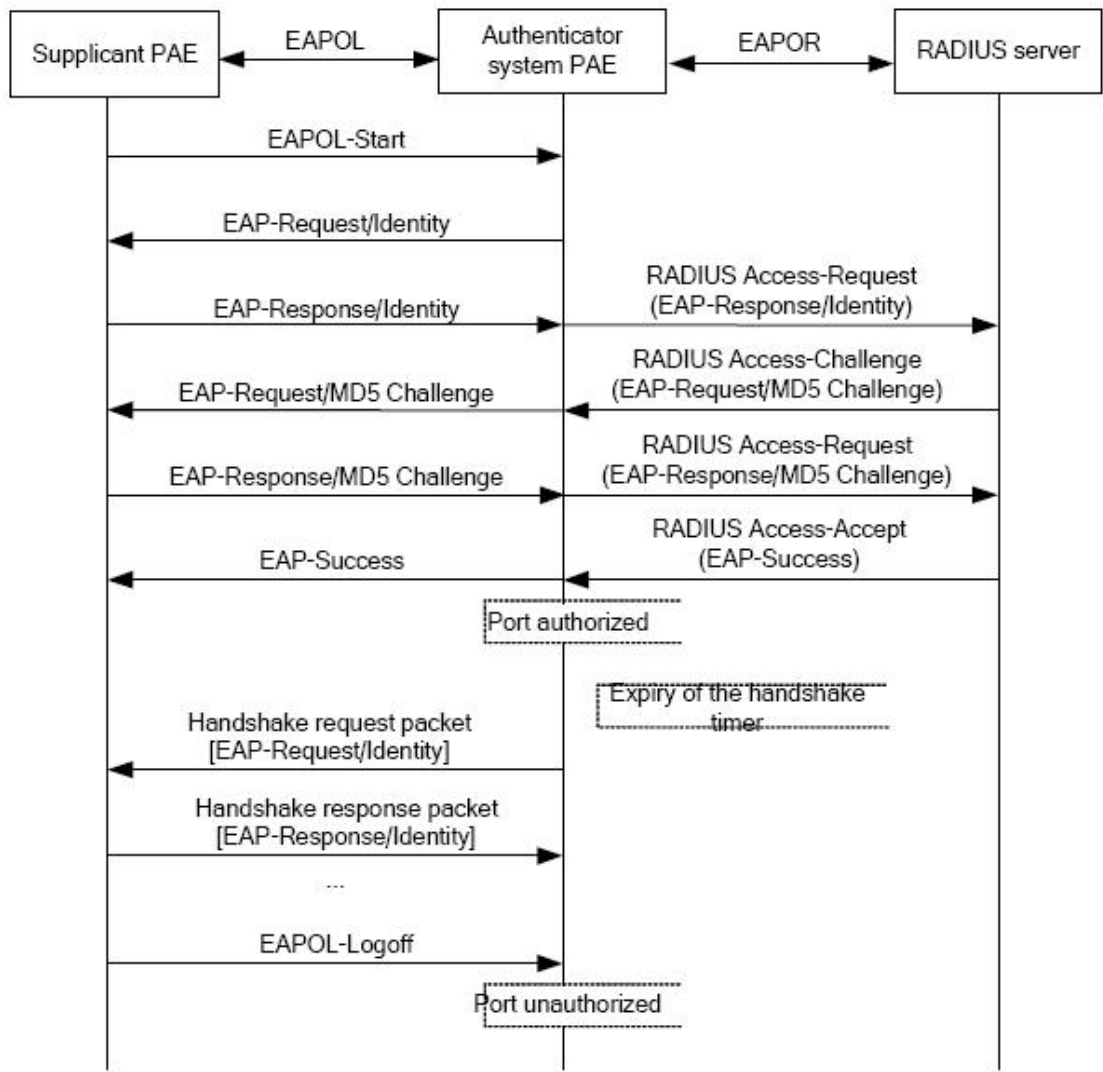


图 2-9 802.1x EAP-MD5 认证流程

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。

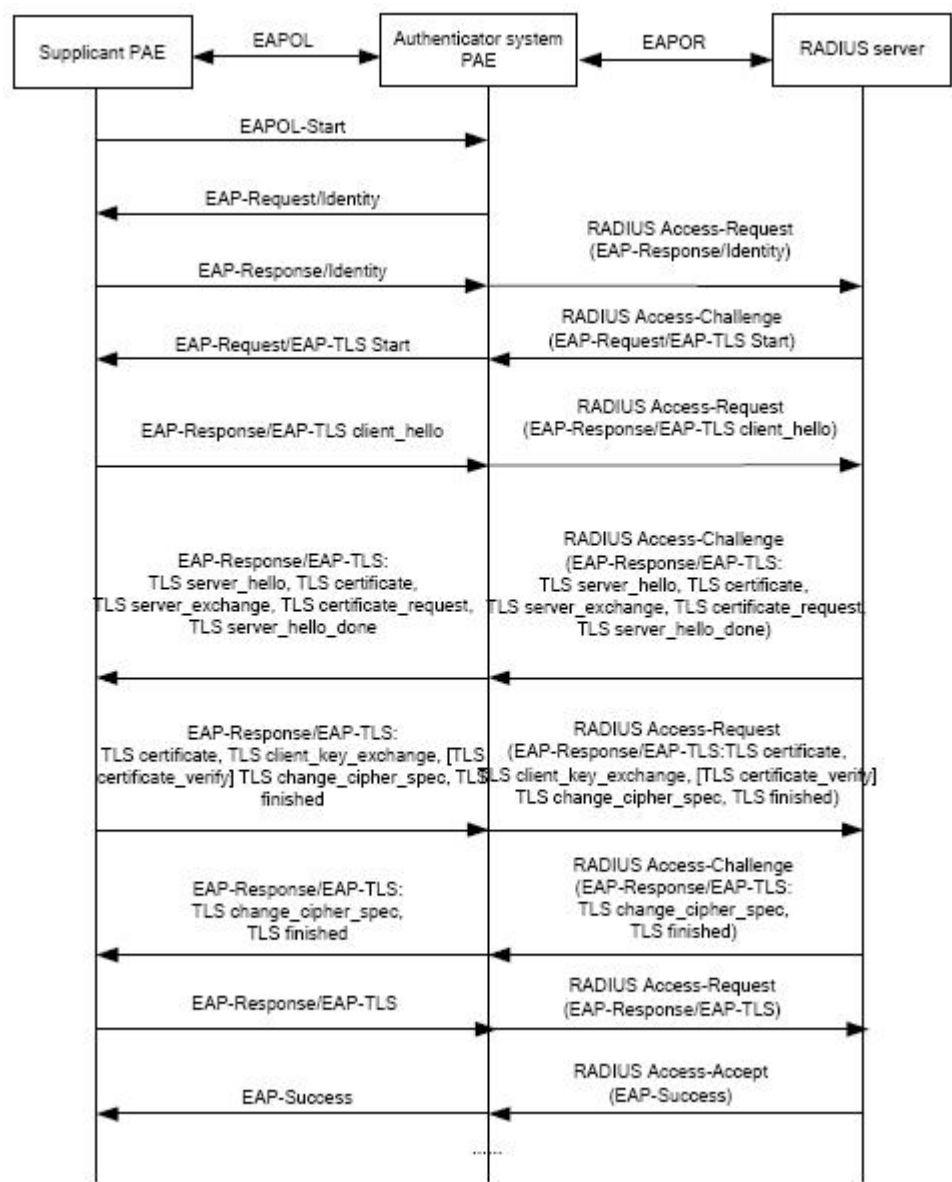


图 2-10 802.1x EAP-TLS 认证流程

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。

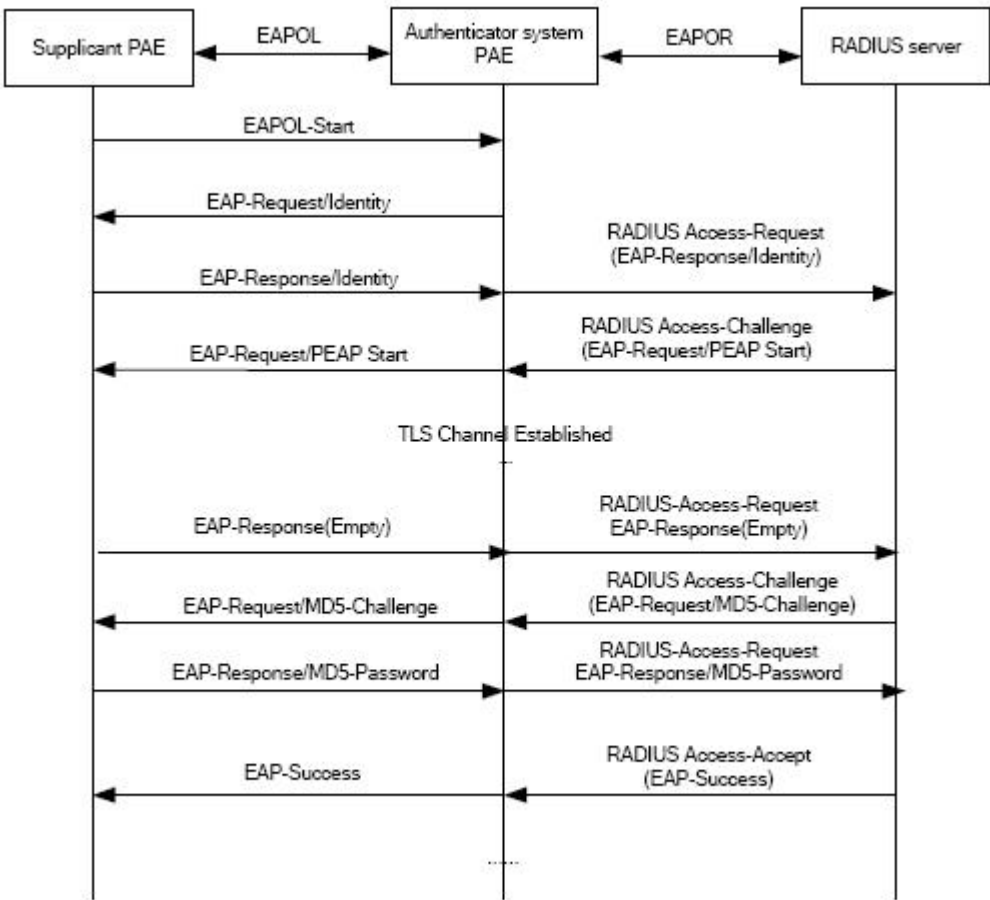


图 2-11 802.1x PEAP 认证流程

2.1.5.2 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。

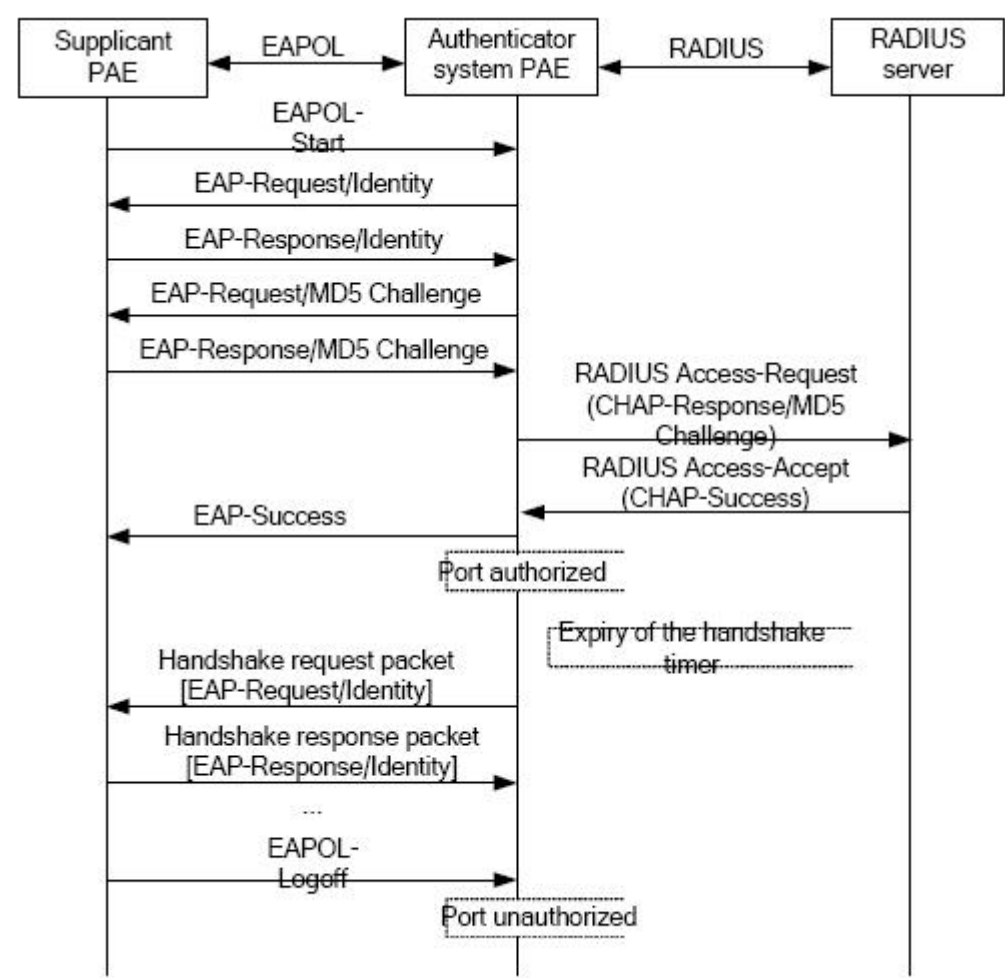


图 2-12 802.1x EAP 终结方式认证流程

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。

2.1.6 802.1x 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：**user-based** 用户数为 **ipv4** 支持 700，**ipv6** 支持 1400；**mac-based** 和交换机的限速值相关，最大可以达到 4000 人，推荐使用认证用户数不超过 2000 人。

2.1.7 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：

- 👉 Tunnel-Type = VLAN (13)
- 👉 Tunnel-Medium-Type = 802 (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 GuestVlan 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。

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. 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
3. 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神州数码私有 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 no 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。

2. 接入控制单元的属性配置

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 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 no 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。

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。

3. 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

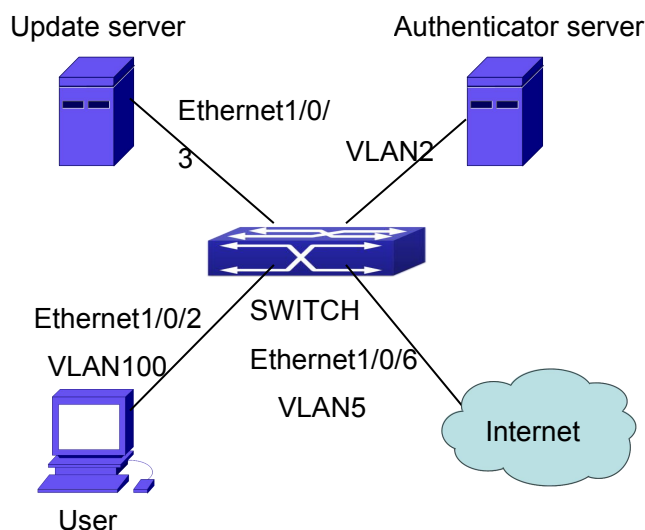


图 2-13: Guest VLAN 网络拓扑结构

如上图所示，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 Ethernet1/0/2 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。

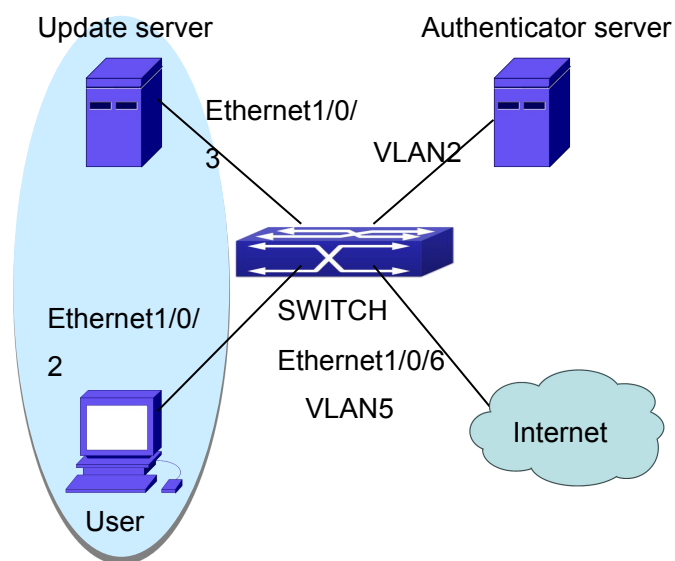


图 2-14: 用户加入 Guest VLAN

如上图所示，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。

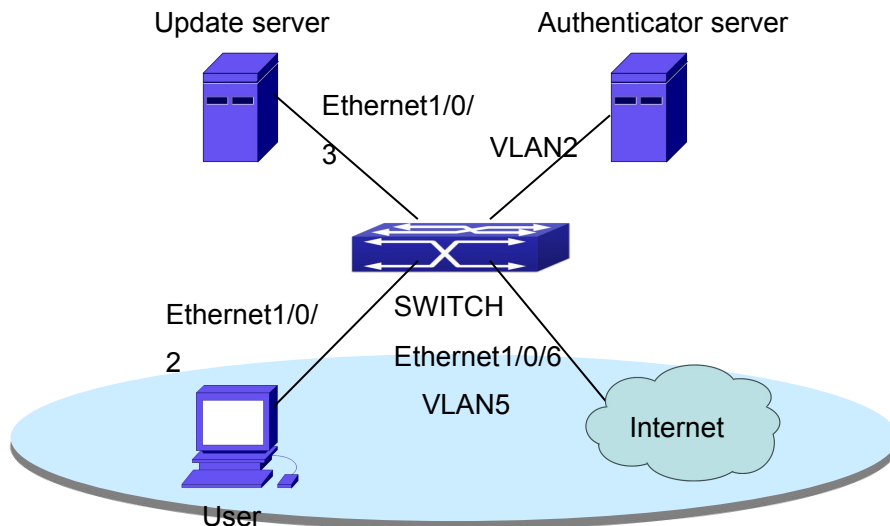


图 2-15：用户上线，VLAN 下发

如上图所示，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

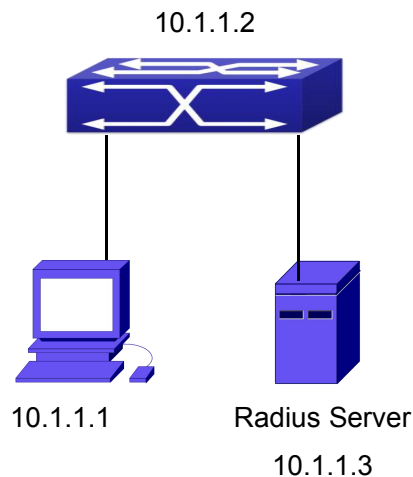


图 2-16 IEEE802.1x 配置举例拓扑图

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

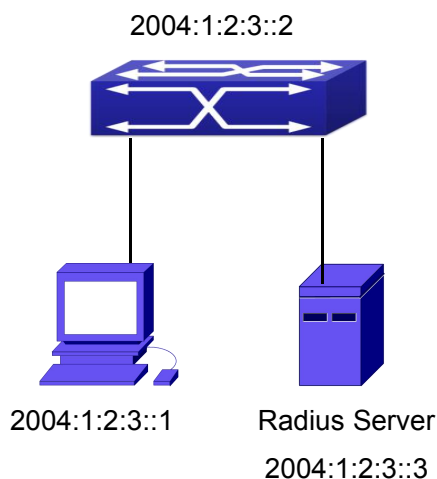


图 2-17 IPv6 Radius 配置举例拓扑图

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-If-Ethernet1/0/2)#dot1x enable
Switch(Config-If-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/0/2)#exit
```

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。

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

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

<code>debug ipv6 nd count</code> <code>no debug ipv6 nd count</code>	VLAN 中 MAC 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

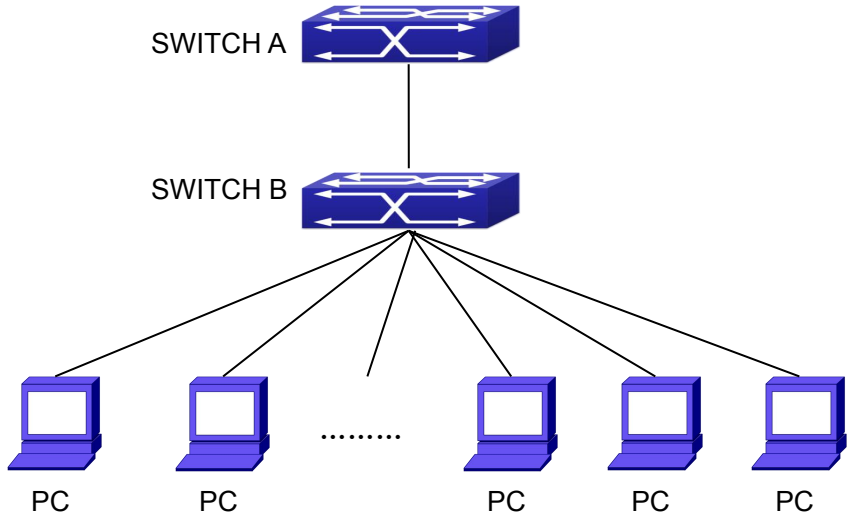


图 3-1 端口、VLAN 中 MAC、IP 数量限制典型配置案例

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

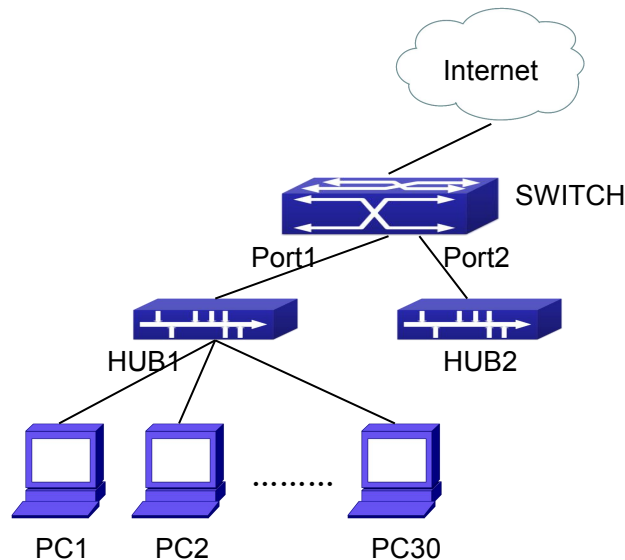


图 4-1 AM 功能典型配置案例

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 TACACS+配置

5.1 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。

5.2 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>	配置 TACACS+服务器认证超时时间；本
no tacacs-server timeout	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>	设置交换设备发送 TACACS+报文的 IP 源
no tacacs-server nas-ipv4	地址。

5.3 TACACS+典型案例

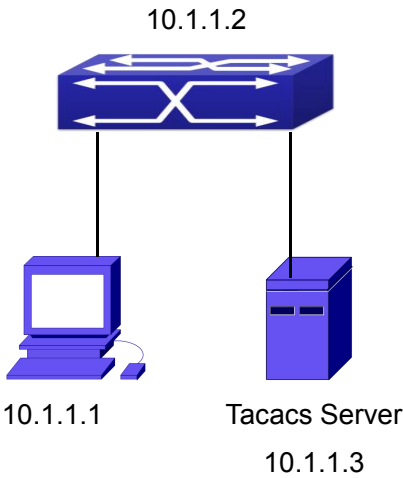


图 5-1 TACACS+配置示意图

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
```

5.4 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：

- ④ 首先应该保证到 TACACS+服务器的物理连接的正确无误；
- ④ 其次，保证接口和链路协议是 UP（使用 `show interface` 命令）；
- ④ 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；
- ④ 然后，确保配置了正确的 TACACS+服务器。

第 6 章 RADIUS 配置

6.1 RADIUS 简介

6.1.1 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。

6.1.2 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：

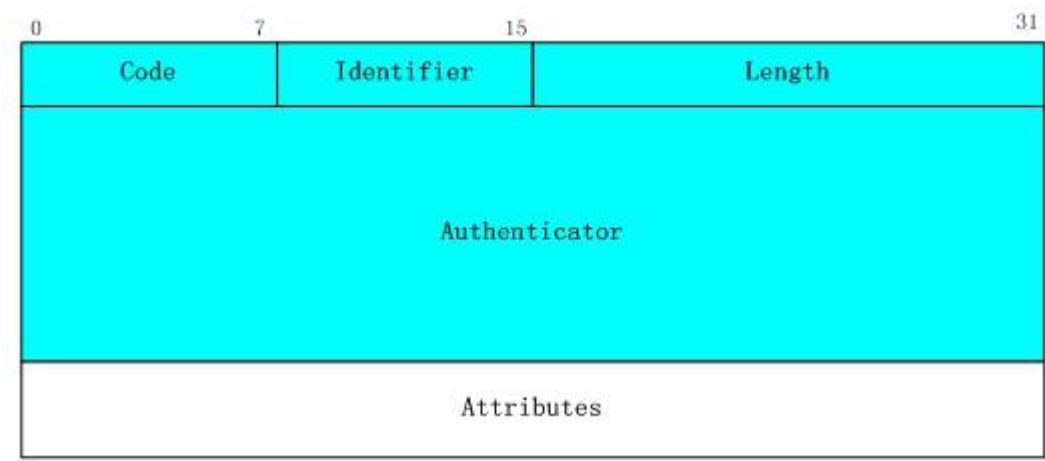


图 6-1 RADIUS 报文结构

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。

6.2 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}] 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。

6.3 RADIUS 典型案例

6.3.1 IPv4 Radius 应用举例

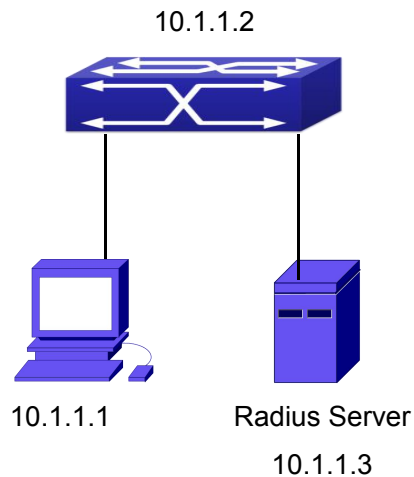


图 6-2 IEEE802.1x 配置举例拓扑图

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
```

6.3.2 IPv6 Radius 应用举例

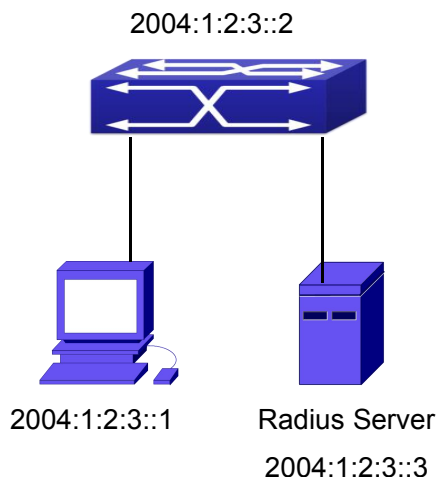


图 6-3 IPv6 RADIUS 配置举例拓扑图

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
```

6.4 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 7 章 SSL 配置

7.1 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)。

7.1.1 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。

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：



7.2 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。

7.3 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。

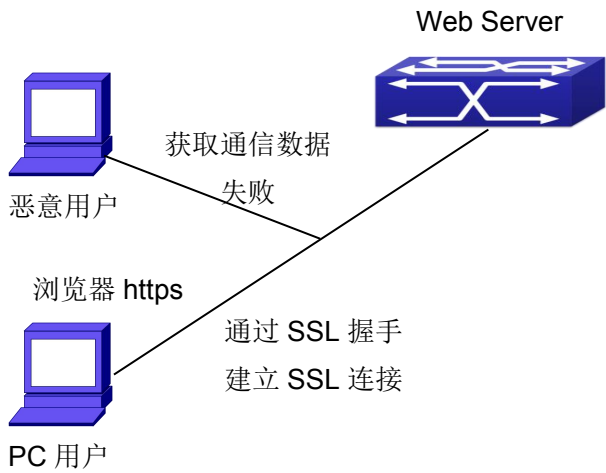


图 7-1 SSL 案例示意图

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
```

7.4 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 8 章 IPv6 安全 RA 配置

8.1 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。

8.2 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。
show ipv6 security-ra [interface <interface-list>]	显示非信任端口和全局安全 RA 是否启动。

8.3 IPv6 安全 RA 典型案例

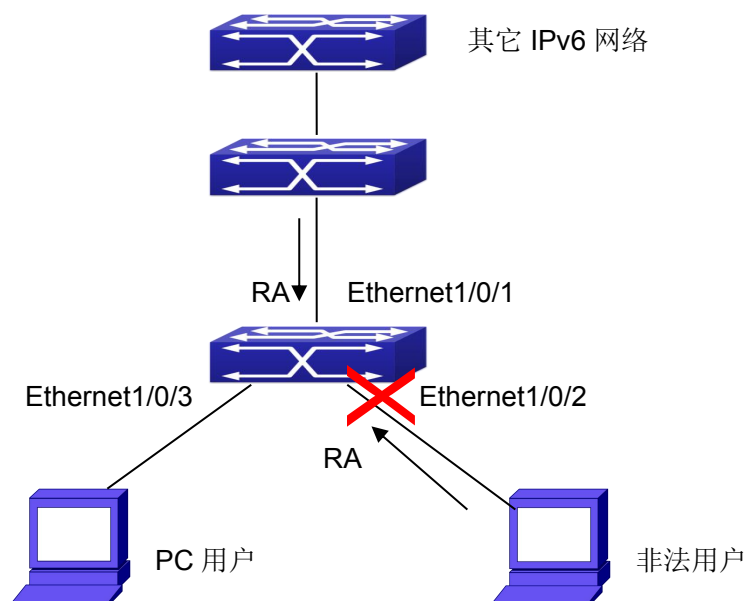


图 8-1 IPv6 安全 RA 案例示意图

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
```

8.4 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 9 章 VLAN-ACL 配置

9.1 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。

9.2 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 vael 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。

9.3 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：

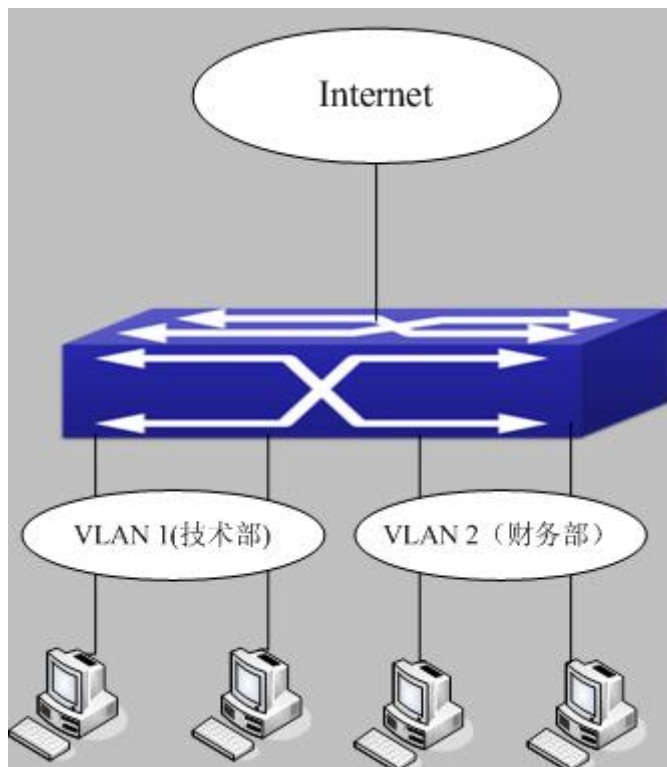


图 9-1 VLAN-ACL 配置案例

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

9.4 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 10 章 MAB 配置

10.1 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）。

10.2 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。

10.3 MAB 举例

案例：
MAB 认证功能典型应用场景如下图所示：

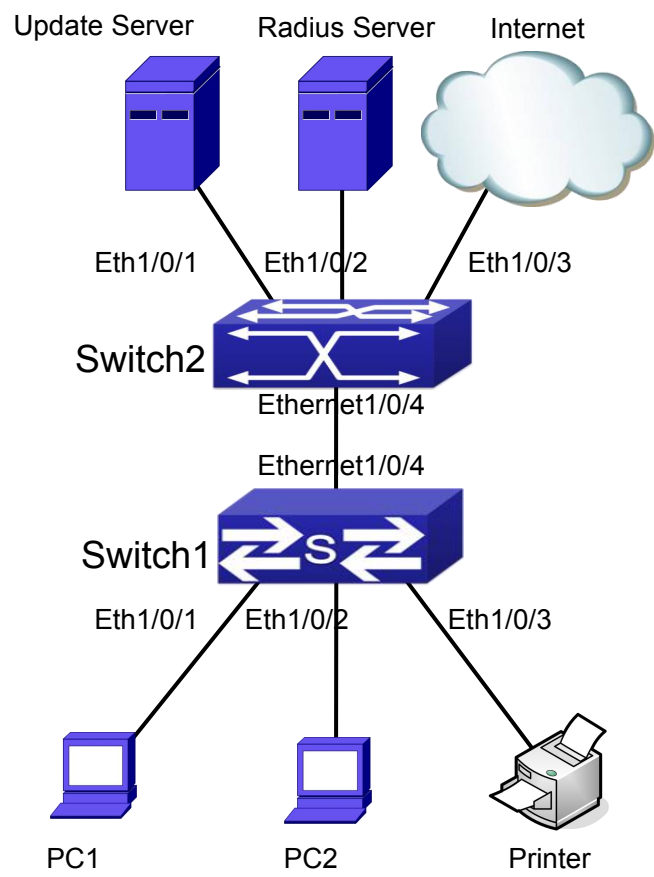


图 10- 1 MAB 应用

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
```

10.4 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。

第 11 章 PPPoE 中间代理配置

11.1 PPPoE Intermediate Agent 介绍

11.1.1 PPPoE 简介

PPPoE 协议,即 Point to Point Protocol over Ethernet,可以看出 PPPoE 协议是把 PPP 协议应用到 Ethernet 上的一种协议。PPP 协议是一种链路层协议,提供了一种点对点的链路层通信方式。PPP 通常是住宅主机拨号链路中所选择的协议,例如链路是电话线拨号。把 PPP 协议应用到 Ethernet 上,即 PPPoE 协议可以使 Ethernet 上的多个主机通过一个或多个简单的桥接设备连接到一个远端的接入集中器上,如果这个远端的接入集中器是宽带接入服务器 (BAS),便可以提供这些主机宽带接入和计费等功能。所以 PPPoE 协议经常被用作 Ethernet 上的宽带接入认证方式。

11.1.2 PPPoE IA 介绍

随着宽带接入技术的快速发展,宽带接入网络发展的越来越大,但是随着宽带接入网络的发展,安全问题逐渐变为公众焦点。在当前接入网络环境下,无论是客户还是接入设备和网络都面临着威胁,尤其是那些来自用户端的威胁。传统以太网的用户不能被精确的识别,追踪以及定位,但是在一个开放的可管理的面向公众的网络,用户身份识别和定位是最基本的特征和要求,例如在提供用户账号登陆的应用时,这种方式能够有效的防止用户账号被盗用,而 PPPoE Intermediate Agent 正提供了这种功能。

PPPoE 协议的工作过程主要分为两个阶段,即发现阶段和会话阶段。发现阶段的作用是得到远端服务器的 Mac 地址,以便建立一个点对点的链接,并与服务器建立一个会话标识 (SESSION ID),在会话阶段使用这个 SESSION ID 进行通信。由于 PPPoE Intermediate Agent 只与发现阶段相关,所以这里只对发现阶段做简要介绍。

PPPoE 协议发现阶段主要分为四步:

1. 主机 (client) 端发送 PADI 报文: PPPoE 发现阶段的第一步,由客户端首先以广播地址为目的地址,广播这个 PADI (PPPoE Active Discovery Initiation) 报文,用以发现二层网络中的接入集中器,注意此消息有可能发送给网络中的多个接入集中器。
2. 接入集中器 (server) 端回应 PADO 报文: PPPoE 发现阶段的第二步,由服务器端根据接收到的 PADI 报文的源 Mac 地址,向主机端回应 PADO (PPPoE Active Discovery Offer) 报文,该报文中会携带接入集中器名和服务名等信息。
3. 主机 (client) 端发送 PADR 报文: PPPoE 发现阶段的第三步,由客户端根据接收到的 PADO 报文,选择一个接入集中器作为将要进行会话的接入集中器,因为在第一步中的 PADI 消息可能发送给网络中的多个接入集中器,所以可能收到多个 PADO 报文,而从这多个接入集中器中进行选择的依据则是主机需要的服务等信息和 PADO 报文中所携带的服务等信息的匹配结果。当选择完接入集中器后便知道将

要进行会话的另一端的 Mac 地址，便向其发送 PADR（PPPoE Active Discovery Request）报文，用于告诉接入集中器有主机进行会话请求。

4. 接入集中器（server）端回应 PADS 报文：PPPoE 发现阶段的第四步，由服务器端根据接收到的 PADR 报文，知道有主机端有会话请求，便创建一个 SESSION ID，并把这个 SESSION ID 通过 PADS（PPPoE Active Discovery Session-confirmation）报文发送给客户端。至此 PPPoE 发现阶段已经完成，因为客户端和服务端都有了 SESSION ID 可以进入会话阶段了。

PPPoE 有一种特殊的报文，即 PADT（PPPoE Active Discovery Terminate）报文，它和上述四种报文具有相同的以太网协议号，即 0x8863，所以它也可以看作是发现阶段的一种报文，但是 PADT 报文可能在会话进行开始之后的任意时间内被发送，主要是用来终止一个 PPPoE 会话的。它可以由主机或接入集中器发送。

PPPoE Intermediate Agent，它提供了一种用户身份识别和定位的功能。其原理是，在 PPPoE 发现阶段，把从客户端主机发出的 PADI 和 PADR 消息，在经过网络接入设备时，打上该设备的接入链路的标识，这样在接入集中器（服务器端，通常是 BAS）上便可以精确的识别该用户的身份以及定位该用户的位置了。

如果直连的接入设备是 LAN Switch，则加入的信息包括：接入交换机的 Mac，Slot ID，Port Index，Vlan ID 等。本功能主要是依据 DSL Forum Technical Report 101，即 Migration to Ethernet-based DSL aggregation 来实现。

11.1.2.1 PPPoE Intermediate Agent 协议交互过程

PPPoE Intermediate Agent 的协议交互过程和 PPPoE 的协议交互过程类似，只是在与 Host 端直连的交换机（Intermediate Agent）上对 PADI 和 PADR 报文加入了接入链路标识而已。具体交互过程如下图所示。

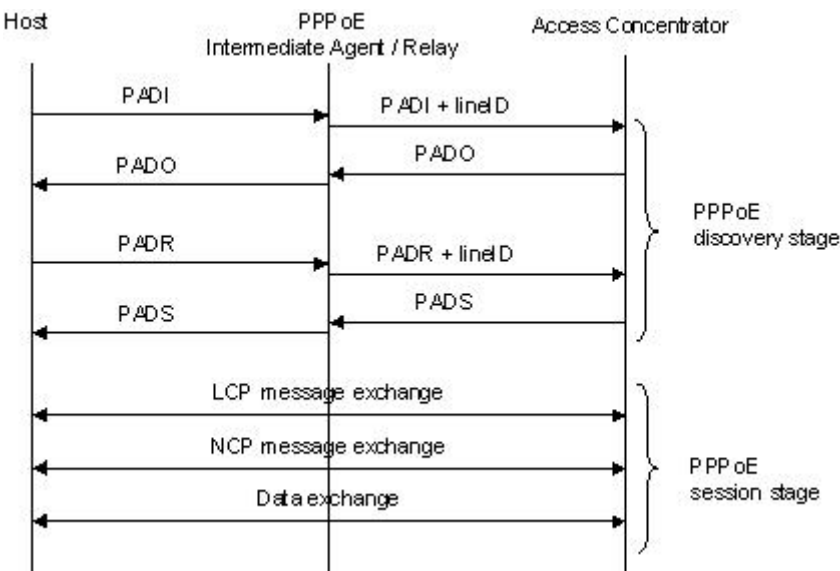


图 11-1 PPPoE IA 协议交互过程

11.1.2.2 PPPoE 报文格式

PPPoE 报文格式如下：



其中各字段含义如下：

Ethernet II 帧的类型域(2byte): 协议规定 PPPoE 协议报文的类型域取值为 0x8863，仅包括 PPPoE 发现阶段的 5 种报文。会话阶段的报文类型域取值为 0x8864。

PPPoE 版本域(4bit): 指明当前 PPPoE 协议版本，规定当前版本必须设置为 0x1

PPPoE 类型域(4bit): 指明协议类型，规定当前版本必须设置为 0x1

PPPoE 代码域(1byte): 指明发送 PPPoE 的报文类型。0x09 代表 PADI 报文，0x07 代表 PADO 报文，0x19 代表 PADR 报文，0x65 代表 PADS 报文，0xa7 代表 PADT 报文。

PPPoE 会话 ID 域(2byte): 指明会话标识

PPPoE 长度域(2byte): 指明所有 TLV 长度和

TLV 类型域(2byte): 一个 TLV 结构代表一个 TAG，类型域则代表 TAG 类型，如下表所示

TLV 长度域(2byte): 指明该 TAG 的数据域的长度。

TLV 数据域(长度不定): 指明该 TAG 的传输的数据

标记类型	标记说明
0x0000	表示PPPOE报文数据域中一串标记的结束，为了保证版本的兼容性而保留，在有些报文中有应用。
0x0101	服务名，主要用来表明网络侧所能提供给用户的一些服务。
0x0102	访问集中器名，当用户侧接收到了AC的响应的PADO报文时，就可获从所携带的标记中获知访问集中器的名子，而且还可以据此来选择相应的访问集中器。
0x0103	主机唯一标识，类似于PPP数据报文中的标识域，主要是用来匹配发送和接收端的，因为对于广播式的网络中会同时存在很多个PPPOE的数据报文。
0x0104	AC-Cookies，主要被用来防止恶意性DOS攻击。
0x0105	销售商的标识符。
0x0110	中继会话ID，对于PPPOE的数据报文也同样可以像DHCP报文一样被中断到另外的AC上终结，这个字段则是用来维护另一个连接的。
0x0201	服务名错误，当请求的服务名不被对端所接受时，会在响应的报文中携带这个标记。
0x0202	访问集中器名出错。
0x0203	一般性错误。

表 11-1 PPPoE 中 TAG 取值类型

11.1.2.3 PPPoE Intermediate Agent vendor tag 结构

下图是 PPPoE IA 最主要的功能，即 PPPoE IA 所要添加的链路标识的结构。

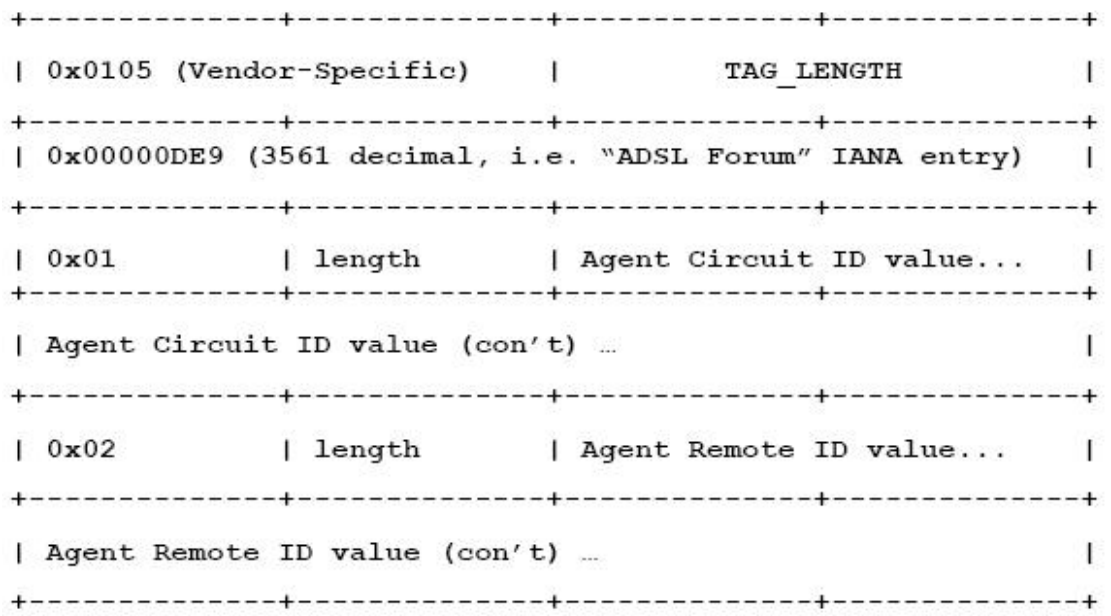


图 11-2 PPPoE IA - vendor tag（每行 4 个字节）

PPPoE IA 添加 tag 的 TLV 类型标识为 0x0105，TAG_LENGTH 是 vendor tag 的长度域； 0x00000DE9 为固定 4 个字节的“ADSL Forum” IANA entry； 0x01 是 Agent Circuit ID 的类型域，length 是其长度域，和 Agent circuit ID value 域； 0x02 是 Agent Remote ID 的类型域，length 是其长度域，和 Agent Remote ID value 域。

PPPoE IA 提供一个默认生成的 circuit ID value，默认生成的 circuit ID 如图所示，其主要包括 5 个字段，其中 ANI（Access Node Identifier）是用户可以配置的，其长度小于 47 个字节；如果没有配置则系统默认为接入交换机的 Mac,占 6 个字节，后面的字段用空格符分隔，“eth”占 3 个字节，和后面的字段用空格符分隔，Slot ID 占 2 个字节，用分隔符“/”分隔且占 1 个字节，Port Index 占 3 个字节，用分隔符“:”分隔且占 1 个字节，Vlan ID 占 4 个字节，这里的所有字段均用 ASCII 码表示。用户也可以根据需要，为每个端口单独配置 circuit id。

ANI (n byte)	Space (1byte)	eth (3 byte)	Space (1byte)	Slot ID (2byte)	/ (1byte)	Port Index (3byte)	: (1byte)	Vlan ID (4byte)
-----------------	-------------------	--------------------	-------------------	---------------------	---------------	---------------------------	---------------	---------------------

图 11-3 Agent Circuit ID value

PPPoE IA 默认生成的 remote ID value 是接入交换机的 Mac。对于 remote ID value 用

户也可以灵活配置，其长度小于 63 个字节。

11.1.2.4 PPPoE Intermediate Agent 的信任端口

PPPoE 发现阶段发送有五种报文，其中 PADI 和 PADR 是由客户端向服务器发送的报文，而 PADO 和 PADS 是由服务器向客户端发送的报文，PADT 报文既可以由服务器发送到客户端，也可以从客户端发送到服务器。

在 PPPoE IA 中，为了安全和减少通讯流量，把连接服务器方向的端口设置为信任端口，把连接客户端的端口设置为非信任端口。对于信任端口可以接收所有报文，对于非信任端口只能接收从客户端发往服务器的 PADI、PADR 和 PADT 报文。为了保证客户端的运行正确，必须把可以连接到服务器的端口设置成信任端口，并且每个接入设备中至少有一个信任端口。

由于 PPPoE IA vendor tag 不能存在于从服务器发往客户端的 PPPoE 报文中，所以这些报文中如果存在 PPPoE IA vendor tag，我们可以选择剥离这些 vendor tag 后转发出去。剥离功能必须在信任端口上配置，非信任端口上也可以开启 vendor tag 剥离功能，但是不起作用。

11.2 PPPoE Intermediate Agent 配置任务序列

- 1. 配置全局开启 PPPoE Intermediate Agent
- 2. 配置端口开启 PPPoE Intermediate Agent

命令	解释
全局配置模式	
pppoe intermediate-agent no pppoe intermediate-agent	开启全局 PPPoE intermediate agent 功能。
pppoe intermediate-agent type tr-101 circuit-id access-node-id <string> no pppoe intermediate-agent type tr-101 circuit-id access-node-id	配置添加的 vendor tag 中 circuit ID 的 access node id 域的值。
pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp sv pv spv} delimiter <WORD> [delimiter <WORD>] no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter	配置添加的 vendor tag 标识中的 circuit-id。

pppoe intermediate-agent type self-defined circuit-id {vlan port id (switch-id (mac hostname) remote-mac) string WORD} no pppoe intermediate-agent type self-defined circuit-id	配置自定义的 circuit-id 形式。
pppoe intermediate-agent type self-defined remoteid {mac vlan-mac hostname string WORD} no pppoe intermediate-agent type self-defined remote-id	配置自定义的 remote-id 形式。
pppoe intermediate-agent delimiter <WORD> no pppoe intermediate-agent delimiter	配置 circuit-id 和 remote-id 各个字段间的分隔符。
pppoe intermediate-agent format (circuit-id remote-id) (hex ascii) no pppoe intermediate-agent format (circuit-id remote-id)	配置 circuit-id 和 remote-id 的表示形式。
端口配置模式	
pppoe intermediate-agent no pppoe intermediate-agent	开启端口 PPPoE intermediate agent 功能。
pppoe intermediate-agent vendor-tag strip no pppoe intermediate-agent vendor-tag strip	设置端口的 vendor tag 剥离功能。
pppoe intermediate-agent trust no pppoe intermediate-agent trust	设置端口为信任端口。
pppoe intermediate-agent circuit-id <string> no pppoe intermediate-agent circuit-id	设置端口的 circuit-id。
pppoe intermediate-agent remote-id <string> no pppoe intermediate-agent remote-id	设置端口的 remote-id。

11.3 PPPoE Intermediate Agent 典型应用

PPPoE IA 的典型应用场景如下：

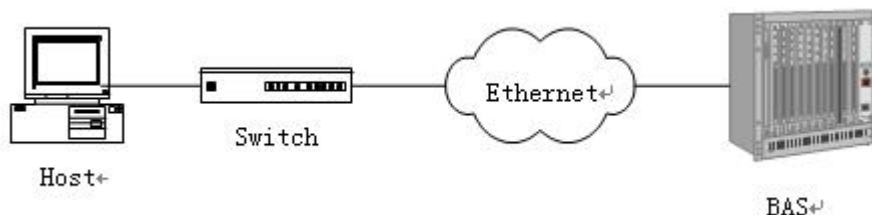


图 11-4 PPPoE IA 典型应用场景

其中 Host 主机和 BAS 服务器端都运行 PPPoE 协议，它们通过二层以太网相连，在与 Host 端直连的交换机开启 PPPoE Intermediate Agent 功能。

典型配置（1）如下：

第一步：在交换机(Switch)上开启全局 PPPoE IA 功能，交换机的 Mac 为 0a0b0c0d0e0f。

```
Switch (config)#pppoe intermediate-agent
```

第二步：配置连接服务器的端口 ethernet1/0/1 为 trust 端口，并且配置 vendor tag 剥离功能。

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
```

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip
```

第三步：在 vlan 1 的端口 ethernet1/0/2 和 vlan 1234 的端口 ethernet1/0/3 上开启端口 PPPoE IA 功能。

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
```

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
```

第四步：配置 pppoe intermediate-agent access-node-id 为 abcd。

```
Switch (config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd
```

第五步：在端口 ethernet1/0/3 上配置 circuit id 为 aaaa，remote id 为 xyz。

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id aaaa
```

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

对于端口 ethernet1/0/2 的 PPPoE 报文添加的 vendor tag 标识中 circuit-id value 为"abcd eth 01/002:0001"，remote-id value 为"0a0b0c0d0e0f"。

对于端口 ethernet1/0/3 的 PPPoE 报文添加的 vendor tag 标识中 circuit-id value 为"aaaa"，remote-id value 为"xyz"。

典型配置（2）如下：

第一步：在交换机(Switch)上开启全局 PPPoE IA 功能。交换机的 Mac 为 0a0b0c0d0e0f。

```
Switch(config)# pppoe intermediate-agent
```

第二步：配置连接服务器的端口 ethernet1/0/1 为 trust 端口，并且配置 vendor tag 剥离功能。

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
```

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip
```

第三步：在 vlan 1 的端口 ethernet1/0/2 和 vlan 1234 的端口 ethernet1/0/3 上开启端口 PPPoE IA 功能。

```
Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent
```

```
Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent
```

第四步：配置 pppoe intermediate-agent access-node-id 为 abcd

```
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd
```

第五步：配置 pppoe intermediate-agent identifier-string 为"efgh"，组合模式为 spv，Slot ID 和 Port ID 的分隔符为"#"，Port ID 和 Vlan ID 的分隔符为"/"。

```
Switch(config)#pppoe intermediate-agent type tr-101 circuit-id identifier-string efgh option  
spv delimiter # delimiter /
```

第六步：在端口 ethernet1/0/2 上配置 circuit-id value 为 bbbb。

```
Switch (config-if-ethernet1/0/2)#pppoe intermediate-agent circuit-id bbbb
```

第七步：在端口 ethernet1/0/3 上配置 remote id 为 xyz。

```
Switch (config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz
```

对于端口 ethernet1/0/2 的 PPPoE 报文添加的 vendor tag 标识中 circuit-id value 为"bbbb"，remote-id value 为"0a0b0c0d0e0f"。

对于端口 ethernet1/0/3 的 PPPoE 报文添加的 vendor tag 标识中 circuit-id value 为"efgh eth 01#003/1234"，remote-id value 为"xyz"。

11.4 PPPoE Intermediate Agent 排错帮助

- 👉 如果要在交换机端口上运行 pppoe intermediate-agent，首先必须在全局打开 pppoe intermediate-agent 开关。在没有打开全局 pppoe intermediate-agent 开关之前，打开端口的 pppoe intermediate-agent 开关是无效的。
- 👉 必须至少配置一个信任端口，并且该端口能连接到服务器。
- 👉 Vendor tag strip 功能必须在信任端口上配置。
- 👉 Circuit-id 的覆盖优先级顺序为：优先级最高的是端口配置 pppoe intermediate-agent circuit-id，优先级次高为 pppoe intermediate-agent identifier-string option delimiter，优先级最低为 pppoe intermediate-agent access-node-id。

第 12 章 SAVI 配置

12.1 SAVI 介绍

SAVI(Source Address Validation Improvement)功能是一种提供节点源地址粒度级的安全验证方式，它通过监听相关协议报文(如 ND 协议，DHCPv6 协议)的交互过程，利用 CPS (Control Packet Snooping)机制，提取节点可信任的信息(如端口，MAC 地址等信息)即锚信息，然后将节点源地址与锚信息进行绑定，并下发绑定信息对应的过滤规则，放行匹配过滤规则的报文，丢弃不匹配过滤规则的报文，从而达到对节点源地址合法性检测的目的。

按照协议报文类型，SAVI 功能主要包括：ND Snooping 功能，DHCPv6 Snooping 功能和 RA Snooping 功能；ND Snooping 功能主要探测 ND 协议报文，主要建立节点以无状态地址配置获取的 IPv6 地址的绑定；DHCPv6 Snooping 功能主要探测 DHCPv6 协议报文，主要建立节点以有状态地址自动配置过程获取的 IPv6 地址的绑定；RA Snooping 功能主要用于防止非法节点冒充路由器发送伪造 RA 报文，以欺骗链路合法性节点的目的。

12.2 SAVI 配置

SAVI 的配置任务序列

- 1. 开启或关闭 SAVI 功能
- 2. 开启或关闭 SAVI 应用场景功能
- 3. 配置 SAVI 绑定功能
- 4. 配置 SAVI max-dad-delay 全局参数
- 5. 配置 SAVI max-dad-prepare-delay 全局参数
- 6. 配置 SAVI max-slaac-life 全局参数
- 7. 配置 SAVI 保护绑定的生存周期参数
- 8. 开启或关闭 SAVI 前缀检查功能
- 9. 配置链路 IPv6 地址前缀功能
- 10. 配置 IPv6 地址过滤表项数目参数
- 11. 配置 SAVI 冲突绑定检测模式
- 12. 开启或关闭端口用户验证功能
- 13. 开启或关闭端口 DHCPv6 报文信任功能
- 14. 开启或关闭端口 ND 报文信任功能
- 15. 配置绑定数目参数

1. 开启或关闭 SAVI 全局功能

命令	解释
全局配置模式	
savi enable	打开全局 SAVI 功能；本命令的 no 操作为关闭全局 SAVI 功能。
no savi enable	

2. 开启或关闭 SAVI 应用场景全局功能

命令	解释
全局配置模式	
savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable no savi ipv6 {dhcp-only slaac-only dhcp-slaac} enable	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。

3. 配置 SAVI 绑定功能

命令	解释
全局配置模式	
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>	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。该命令可在 savi enable, slaac-only enable, dhcp-only enable 和 dhcp-slaac enable 任何一个全局功能下进行配置。

4. 配置 SAVI max-dad-delay 全局参数

命令	解释
全局配置模式	
savi max-dad-delay <max-dad-delay> no savi max-dad-delay	配置 SAVI 绑定处于 DETECTION 状态最大生存周期，本命令 no 操作为恢复默认值。

5. 配置 SAVI max-dad-prepare-delay 全局参数

命令	解释
全局配置模式	
savi max-dad-prepare-delay <max-dad-prepare-delay> no savi max-dad-prepare-delay	配置 SAVI 绑定重新探测的最大生存周期，本命令 no 操作为恢复默认值。

6. 配置 SAVI max-slaac-life 全局参数

命令	解释
全局配置模式	
savi max-slaac-life <max-slaac-life> no savi max-slaac-life	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。

7. 配置 SAVI 保护绑定的生存周期参数

命令	解释
全局配置模式	
savi timeout bind-protect <protect-time> no savi timeout bind-protect	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。

8. 开启或关闭 SAVI 前缀检查功能

命令	解释
全局配置模式	
ipv6 cps prefix check enable no ipv6 cps prefix check enable	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。

9. 配置链路 IPv6 地址前缀功能

命令	解释
全局配置模式	
ipv6 cps prefix <ip-address> vlan <vid> no ipv6 cps prefix <ip-address>	手工配置一条 IPv6 地址链路前缀，本命令 no 操作为删除一条配置的 IPv6 地址链路前缀。

10. 配置 IPv6 地址过滤表项数目参数

命令	解释
全局配置模式	
savi ipv6 mac-binding-limit <limit-num> no savi ipv6 mac-binding-limit	配置同一 MAC 地址对应的 SAVI 动态绑定数目；no 操作为恢复默认值。注意：该配置绑定表项限制仅适用于动态绑定数目，而不限静态绑定的数目。

11. 配置 SAVI 冲突绑定检测模式

命令	解释
全局配置模式	
savi check binding <simple probe> mode no savi check binding mode	配置冲突绑定检查模式；no 命令为删除配置的冲突绑定的检查模式。

12. 开启或关闭端口用户验证功能

命令	解释
----	----

端口配置模式	
savi ipv6 check source [ip-address mac-address ip-address mac-address] no savi ipv6 check source	开启用户控制验证功能，本命令的 no 操作作为关闭用户验证功能。

13. 开启或关闭端口 DHCPv6 报文信任功能

命令	解释
端口配置模式	
ipv6 dhcp snooping trust no ipv6 dhcp snooping trust	开启端口 DHCPv6 报文信任功能，本命令的 no 操作作为关闭端口 DHCPv6 信任功能，端口由信任端口转变为非信任端口。

14. 开启或关闭端口 ND 报文信任功能

命令	解释
端口配置模式	
ipv6 nd snooping trust no ipv6 nd snooping trust	开启端口为 slaac trust 和 RA trust 功能，本命令的 no 操作作为删除 slaac trust 和 RA trust 功能。

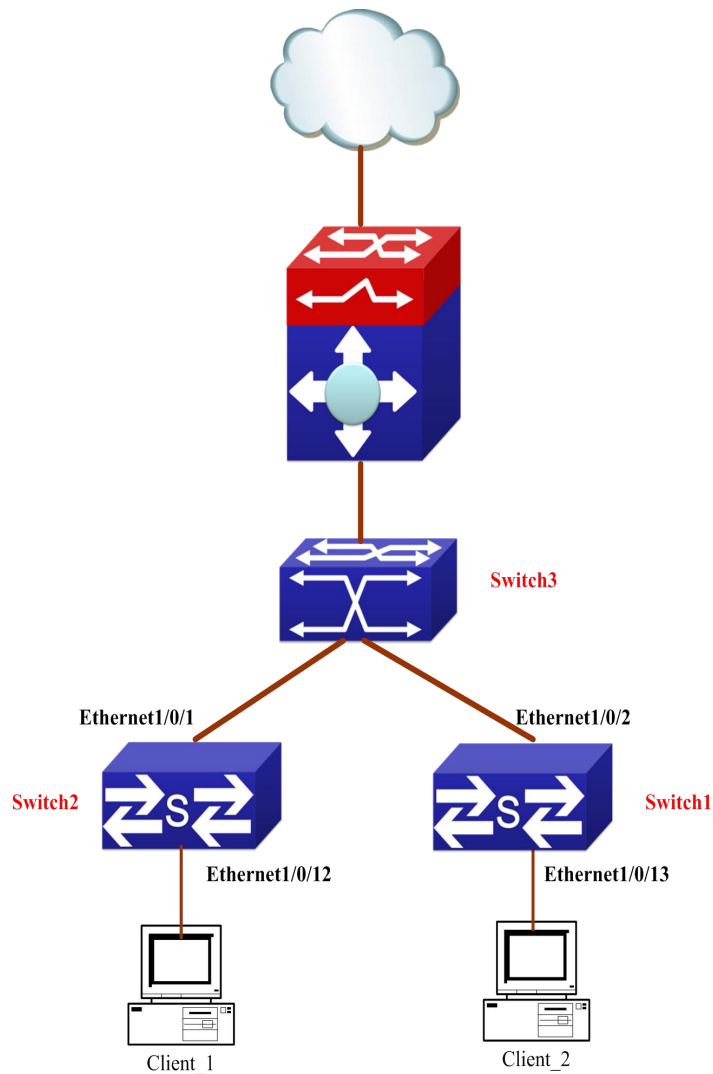
15. 配置绑定数目参数

命令	解释
端口配置模式	
savi ipv6 binding num <limit-num> no savi ipv6 binding num	配置端口的绑定数目，本命令的 no 操作作为还原默认值。注意：该端口绑定数据限制仅包括动态绑定数目，不对静态绑定数目进行限制。

12.3 SAVI 典型应用

在实际工程应用中，SAVI 功能一般应用在接入层交换机中，对直连链路上的用户节点进行源地址合法性检测；SAVI 功能典型的应用场景主要有四种：DHCP-Only 场景、Slaac-Only 场景、DHCP-Slaac 场景和静态绑定场景。在具体的网络环境中，用户可根据实际需求选择对应的场景。在双栈网络中，SAVI 功能也可以和 IPv4 的 DHCP snooping 配合使用，同时实现 IPv4 和 IPv6 源地址验证。

SAVI 功能典型的应用网络拓扑环境



其中 Client_1 和 Client_2 代表两台不同用户的 PC 机, 每台 PC 机都已安装 IPv6 协议, 直连交换机 Switch1 和 Switch2, 直连端口分别为 Ethernet1/0/12, Ethernet1/0/13, 并开启 SAVI 的源地址检查功能。Switch1 和 Switch2 上联端口分别为 Ethernet1/0/1, Ethernet1/0/2, 并开启 DHCP 报文信任和 ND 报文信任功能。汇聚交换机 Switch3 开启 DHCPv6 服务器功能和路由公告功能。

SAVI DHCP-SLAAC 组合场景配置步骤:

```
Switch1>enable
```

```
Switch1#config
```

```
Switch1(config)#savi enable
```

```
Switch1(config)#savi ipv6 dhcp-slaac enable
```

```
Switch1(config)#savi check binding probe mode
```

```
Switch1(config)#interface ethernet1/0/1
```

```
Switch1(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust
```

```
Switch1(config-if-ethernet1/0/1)#ipv6 nd snooping trust
```

```
Switch1(config-if-ethernet1/0/1)#exit
```

```
Switch1(config)#interface ethernet1/0/12-20
Switch1(config-if-port-range)#savi ipv6 check source ip-address mac-address
Switch1(config-if-port-range)#savi ipv6 binding num 4
Switch1(config-if-port-range)#exit
Switch1(config)#exit
Switch1#write
```

12.4 SAVI 排错帮助

在确保 SAVI 客户机硬件、线缆等没有问题的前提下，检查可能存在的情况和建议的解决方法：

- ☞ 若交换机开启 SAVI 功能后，没有正确的过滤 IPv6 报文，首先检查交换机上 SAVI 全局功能是否已开启，若没有开启，首先开启 SAVI 全局功能；然后根据实际的应用场景，启用对应的 SAVI 场景全局功能，并同时开启端口验证功能；
- ☞ 若交换机开启 SAVI 功能后，客户端无法正确的获取上联 DHCPv6 服务器的分配的 IPv6 地址，首先检查开启交换机上联 DHCPv6 服务器的接口是否配置 DHCP 端口信任功能，若没有启用，启用 DHCP 端口信任功能；
- ☞ 若交换机开启 SAVI 功能后，无法建立新增用户节点的绑定，首先检查用户直连交换机端口是否配置端口绑定数目限制功能，是否绑定数目已达到最大值；若已超过端口最大绑定数目限制，建议配置较大的端口绑定数目限制；
- ☞ 若配置较大端口绑定数目限制后，仍无法建立新增用户节点的绑定，则应检查用户直连交换机端口是否配置同一 MAC 地址对应绑定数目限制功能，同一 MAC 地址对应的绑定数目是否已达到最大值；若已超过最大绑定数目限制，建议配置较大的绑定数目限制。

第 13 章 Captive Portal 认证

13.1 Captive Portal 认证配置

13.1.1 Captive Portal 认证介绍

认证功能是为管理和控制使用网络资源的用户的一种方法。认证功能将客户端的认证信息按照一定的原则存储在认证服务器中，当用户需要使用网络资源时，**captive portal** 功能将用户的网络请求重定向到认证服务器上，这时需要用户提供被允许的用户名和密码等信息，由认证服务器对用户提供的信息进行判断，以决定是否允许该用户使用网络资源。交换机在认证功能中主要起着传递用户和认证服务器之间通信的作用。通过在交换机上进行配置使得客户端可以与认证服务器进行连接和沟通，并且在认证服务器对客户端信息判断完成后将认证结果和相应处理推向用户。认证功能是建立在重定向功能基础之上的。

重定向功能是一种将原请求重新连接到设定好的地点后再进行后续操作的功能。该功能是在交换机接收到客户端的请求后，将客户端的请求转到一个已经设定好的地址上，之后的操作由客户端和重定向之后的地址进行操作，以此完成某些特定的功能和操作。该操作可以实现达到管理和监控用户的目的。客户端被重定向 **portal** 认证界面，需要用户填写用户名和密码，只有当该用户名和密码通过认证后才允许用户使用网络资源。**Portal** 认证方式可以实现对不同类型用户的不同控制策略。

多 **portal server** 功能是为不同的 **CP configuration** 配置不同的外置 **portal server** 的一种方法。绑定在不同 **CP configuration** 下的端口配置了不同 **portal server** 之后就可以各自通过自身绑定的 **portal server** 来推出重定向页面。最多可以配置 10 台外置 **portal** 服务器。每个 **cp configuration** 可以绑定一台 **portal** 服务器。

13.1.2 Captive Portal 认证配置

认证功能配置任务序列如下：

1. 打开或关闭 **captive portal** 认证功能
2. 配置 **captive portal** 重定向功能
 - 1) 设置或删除 **portal** 服务器名称
 - 2) 配置用户例程
 - 3) 配置重定向地址
 - 4) 配置重定向 **url** 头部
 - 5) 设置或删除 **radius** 服务器名称
 - 6) 配置绑定或者解除 **portal** 服务器
 - 7) 配置 **url** 携带 **ac-name** 参数
 - 8) 配置 **url** 携带 **ssid** 参数

- 9) 配置 url 携带 nas-ip 参数
- 3. 配置 AAA 功能
 - 1) 打开使能或禁止 AAA 功能
 - 2) 配置 RADIUS 认证服务器组名称
- 4. 配置 RADIUS 认证服务器
 - 1) 配置 RADIUS 服务器密钥
 - 2) 配置 RADIUS 认证服务器地址
- 5. 将 portal 规则绑定到端口下

1. 打开或关闭 captive portal 认证功能

命令	解释
Captive portal 配置模式	
enable disable	全局打开或关闭 captive portal 功能。

2. 配置 captive portal 重定向功能

命令	解释
Captive Portal 配置模式	
external portal-server server-name <name> {ipv4 ipv6} <ipaddr> [port <1-65535>] no external portal-server {ipv4 ipv6}server-name <name>	配置或删除外置 portal 服务器。
nas-ip4 <A.B.C.D>	配置 nas-ip 地址
configuration <cp-id> no configuration <cp-id>	配置与删除不同类型用户的 portal 例程。该例程可以配置 10 种不同的例程。
Captive Portal Instance 配置模式	
redirect url-head <word> no redirect url-head	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。
radius-auth-server <server-name> no radius-auth-server	设置或删除 radius 认证服务器名称。
portal-server {ipv4 ipv6} <name> no portal-server {ipv4 ipv6}	绑定或解除绑定 portal 服务器名称。
enable disable	打开或关闭某个 portal 例程。

ac-name <word> no ac-name	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。
redirect attribute ssid name <word> no redirect attribute ssid name	配置在重定向 url 中携带的 ssid 参数名称。本命令的 no 形式为恢复重定向 url 中携带的 ssid 参数名称为默认值。
redirect attribute nas-ip enable no redirect attribute nas-ip enable	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。
redirect attribute nas-ip name <word> no redirect attribute nas-ip name	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。

3. 配置 AAA 功能

命令	解释
全局配置模式	
aaa enable no aaa enable	使能或禁止 AAA 功能
aaa group server radius <word> no aaa group server radius <word>	设置或删除设置 AAA 功能的 RADIUS 名称。

4. 配置 RADIUS 认证服务器

命令	解释
全局配置模式	
radius-server key <word> no radius-server key	设置或删除 RADIUS 服务器密钥。
radius-server authentication host <A.B.C.D> no radius-server authentication host <A.B.C.D>	配置或删除 RADIUS 认证服务器地址。

5. 开启/关闭端口 portal 功能

命令	解释
config 配置模式	

vlan-pool <1-255> <WORD> no vlan-pool <1-255>	配置或者删除地址池（可选）。
端口模式	
portal enable configuration <id> [vlan-pool WORD] no portal enable [vlan-pool WORD]	开启端口 portal 认证功能，指定端口绑定的实例号，并且可以指定哪些 VLAN 使能 portal，如果不指定 vlan，则默认所有 vlan 使能 portal。本命令的 no 形式为关闭端口 portal 认证功能。（必选）

13.1.3 Captive Portal 认证举例

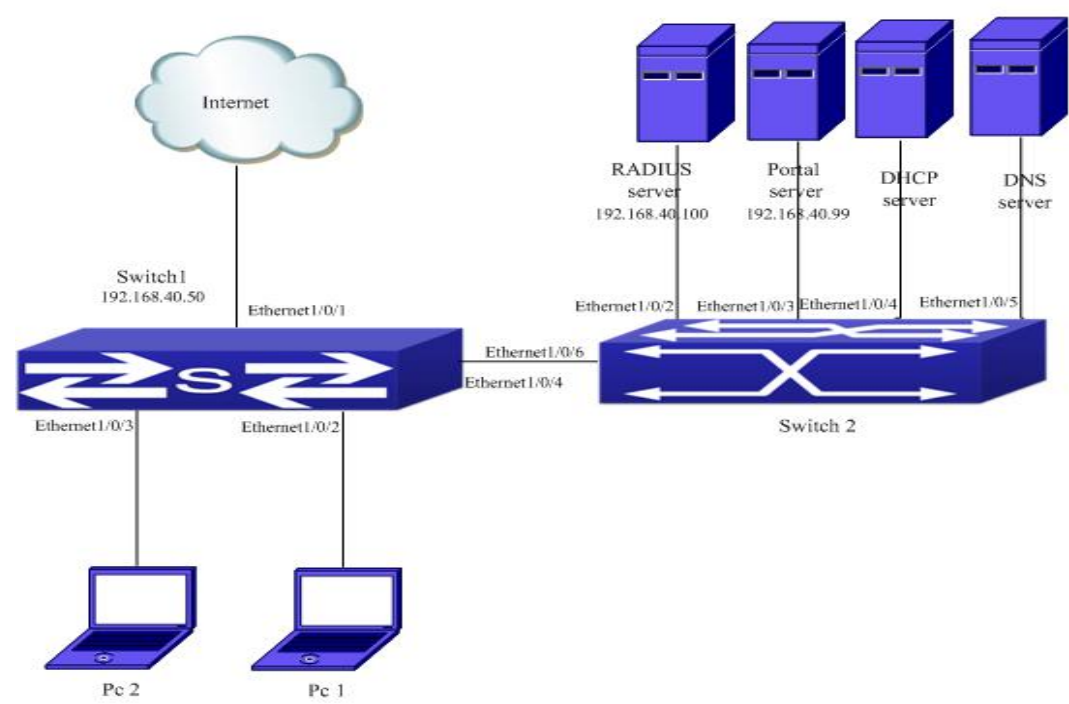


图 13-1 认证功能配置

如图所示，pc1 为终端用户，上面有 http 浏览器，但没有任何 802.1x 认证客户端，pc1 想要通过 portal 认证上网。

交换机是 Switch1 为接入设备，上面配置了计费服务器的地址为 RADIUS 服务器的 IP 和端口，打开了计费功能。其中 Ethernet1/0/2 和 pc1 相连，端口打开了 portal 认证功能，配置了重定向的地址为 portal 服务器的 IP 和端口，因此端口 Ethernet1/0/2 禁止所有的流量，只放行 dhcp/dns/arp 报文通过。

交换机 Switch2 为汇聚交换机，Ethernet1/0/2 与后台 radius 服务器互通，Ethernet1/0/3

与 portal 服务器互通。Radius 服务器的地址为 192.168.40.100，portal 服务器的地址为 192.168.40.99。Ethernet1/0/4 连接的是 DHCP 服务器，Ethernet1/0/5 连接的是 DNS 服务器。Ethernet1/0/6 为 trunk 口，与 Switch 1 的 trunk 口 Ethernet1/0/4 相连。

配置 radius 服务器：

```
switch (config)#radius-server key 0 test
switch (config)#aaa group server radius radius_aaa_1
switch (config-sg-radius)# server 192.168.40.100
```

portal 全局开启认证功能相关的配置如下：

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
Switch(config)#free-resource 1 destination ipv4 192.168.40.99/32
Switch(config)# vlan-pool 1 2-10
```

portal实例下Portal功能、配置Portal Server服务器等信息：

```
Switch (config)#captive-portal
Switch (config-cp)#enable
Switch(config-cp)# nas-ipv4 192.168.40.50
Switch(config-cp)# external portal-server server-name abc ipv4 192.168.40.99
Switch (config-cp)# configuration 1
Switch (config-cp-instance)#name helix4
Switch (config-cp-instance)#radius-auth-server abc99
Switch (config-cp-instance)# redirect attribute nas-ip enable
Switch (config-cp-instance)#redirect attribute nas-ip name kk
Switch (config-cp-instance)#ac-name helix4
Switch (config-cp-instance)#redirect url-head http://192.168.40.99/a70.htm
Switch (config-cp-instance) # portal-server ipv4 abc
```

端口上开启 portal 功能

```
Switch (config)# interface ethernet1/0/2
Switch (config-if-ethernet1/0/2)#portal enable configuration 1 vlan-pool 1
```

13.1.4 Captive Portal 认证排错帮助

当在使用重定向功能和 Captive Portal 功能过程中遇到问题，请检查是否是如下原因：

- ☞ 是否启动了 captive portal 功能以及是否打开了 portal 的 configuration 开关，这两项都应当打开，否则 captive portal 功能不能正常使用，客户端也不能重定向到指定页面。
- ☞ AAA 模块的认证服务器名称与 captive portal 配置的认证服务器名称相同。

☞ pc 和交换机相连的端口上是否打开了 portal 认证功能。

13.2 计费功能配置

13.2.1 计费功能介绍

计费功能是为对网络中的用户使用网络资源进行监控和计费的功能。客户端在未通过 captive portal 认证功能之前是无法访问网络资源的，只有通过了 portal 认证才能访问网络资源，可以定义用户的会话时长以控制用户使用网络资源的时间和流量等信息。

13.2.2 计费功能配置

计费功能配置任务序列如下：

1. 配置 RADIUS 计费服务器
 - 1) 设置或删除计费服务器地址
2. 配置 AAA 计费功能
 - 1) 打开或关闭计费服务功能
3. 配置 captive portal 计费功能
 - 1) 阻塞或解除阻塞 portal 功能
 - 2) 设置或删除 captive portal 配置名称
 - 3) 打开或关闭 captive portal 计费功能
 - 4) 配置或删除 captive portal 计费服务器名称
 - 5) 配置或删除 captive portal 会话时长

1. 配置 RADIUS 计费服务器

命令	解释
全局配置模式	
radius-server accounting host <A.B.C.D> no radius-server accounting host <A.B.C.D>	设置或删除计费服务器地址。

2. 配置 AAA 计费功能

命令	解释
全局配置模式	
aaa-accounting enable no aaa-accounting	打开或关闭计费服务功能。

3. 配置 captive portal 计费功能

命令	解释
Captive portal 配置模式	
block no block	阻塞或解除阻塞 portal 功能
name <word> no name	设置或删除 captive portal 配置名称。
radius accounting no aaa-accounting	打开或关闭 captive portal 计费服务功能。
radius-acct-server <word> no radius-acct-server	配置或删除 captive portal 计费服务器名称。
session-timeout <0-86400> session-timeout	配置或删除 captive portal 会话时长。

13.2.3 计费功能举例

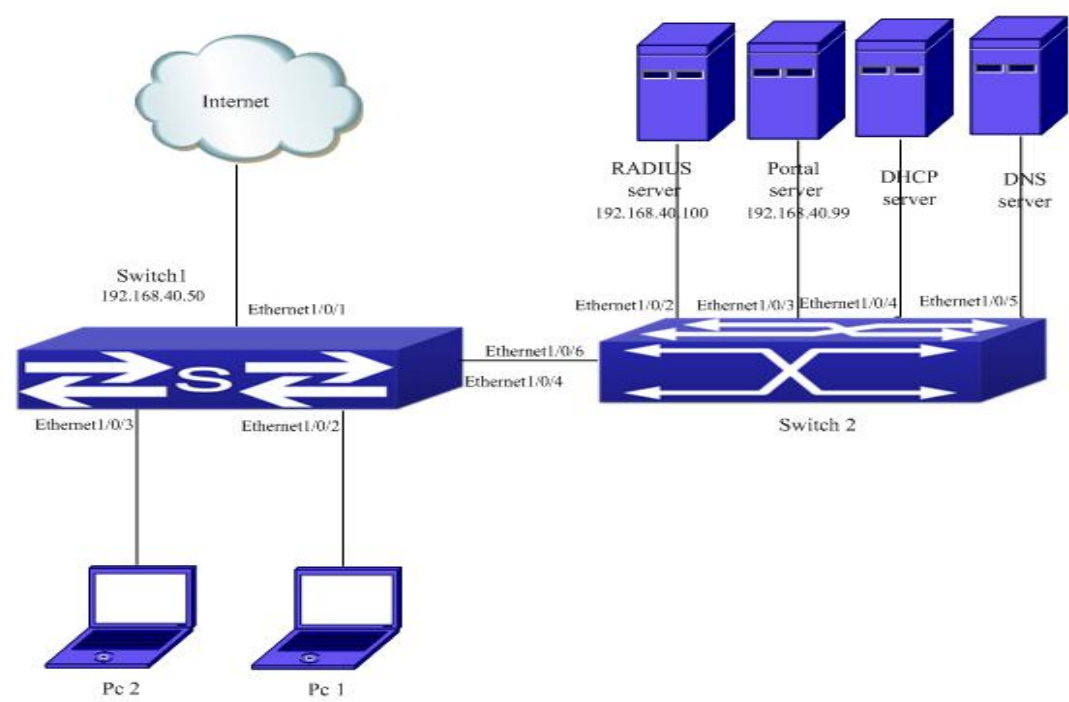


图 13-2 计费功能配置图

1. 在 switch1 上配置 AAA 计费功能

Switch1 的 AAA 配置：

```
switch 1(config)# aaa enable
switch 1(config)# aaa-accounting enable
switch 1(config)# radius-server accounting host 192.168.40.100
```

```
switch1 (config)#radius-server key 0 test
switch1 (config)#aaa group server radius abc99
switch (config-sg-radius)# server 192.168.40.100
2. 在 switch1 上配置 captive portal 计费功能
Switch 1(config)#captive-portal
Switch 1(config-cp)#enable
Switch1 (config-cp)# configuration 1
Switch1 (config-cp-instance)#radius accounting
Switch1 (config-cp-instance)# radius-acct-server abc99
```

13.2.4 计费功能排错帮助

- 当在使用计费功能过程中遇到问题，请检查是否是如下原因：
- ☞ 是否启动了 captive portal 功能以及是否打开了 portal 的 configuration 开关，这两项都应当 enable，否则 captive portal 功能不能正常使用。
 - ☞ AAA 模块的认证服务器名称与 captive portal 配置的认证服务器名称相同。

13.3 Free-resource 功能配置

13.3.1 Free-resource 功能介绍

Free-resource 功能是 captive portal 模块中实现访问免费资源规则的方法，通过配置 free-resource 规则，可以让某些特定的客户端不通过 portal 认证就可以直接访问特定的网络资源。

13.3.2 Free-resource 功能配置

1. 配置 free-resource 规则

命令	解释
config 配置模式	
free-resource destination {ipv4 A.B.C.D/M ipv6 X:X:X:X/M} [no] free-resource destination {ipv4 A.B.C.D/M ipv6 X:X:X:X/M}	配置或删除 free-resource 规则。

13.3.3 Free-resource 功能举例

案例：

搭建环境如下图所示，IP 为客户端 client1 所在的地址段，目的 IP 为客户端想要访问的资源的地址段，指定 RADIUS Server 1 为认证服务器，客户端 client1 和 client2 可以访问该免费资源 3.1.1.0/24，不会被重定向到认证服务器上，直接就可以成功访问。

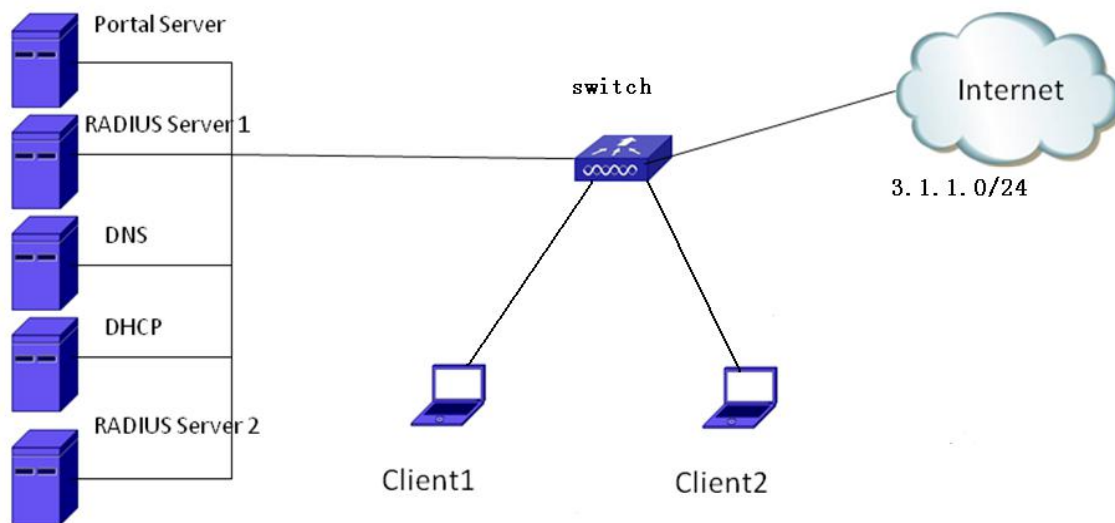


图 13-3 多 portal server 功能配置

配置免费资源步骤：

```
Switch1 (config)# free-resource destination ipv4 3.1.1.0/24
```

13.3.4 Free-resource 功能排错帮助

当在使用重定向功能过程中遇到问题，请检查是否是如下原因：

- ☞ 是否正确启动了 captive portal 功能以及是否打开了 portal 的 configuration 开关，这两项都应当打开，否则多 portal server 功能不能正常使用，客户端也不能重定向到指定页面。
- ☞ Client 和交换机互连的端口是否开启了 portal 规则。

13.4 认证白名单功能配置

13.4.1 认证白名单功能介绍

认证白名单功能是为对网络中某些特殊的用户使用的，管理员可以设置一些用户使其连接到网络之后不需要通过认证即可使用网络资源，但是管理员需要获得该类用户的 mac 地址才能使用该功能，同时具有该权限的用户所使用的网络资源不需要不給计费，因此该类用户的权限属于高级用户类型。

13.4.2 认证白名单功能配置

1. 配置具有认证白名单功能权限的用户的 mac

命令	解释
config 配置模式	
free mac < MACADD><MACMASK>	设置或删除可以免认证的 mac 地址。
no free mac < MACADD><MACMASK>	

13.4.3 认证白名单功能举例

如图所示，client1 和 client2 为终端用户，和交换机相连的端口开启了 portal 认证，但是这两个用户为高级用户，不需要认证，就可以正常访问资源。

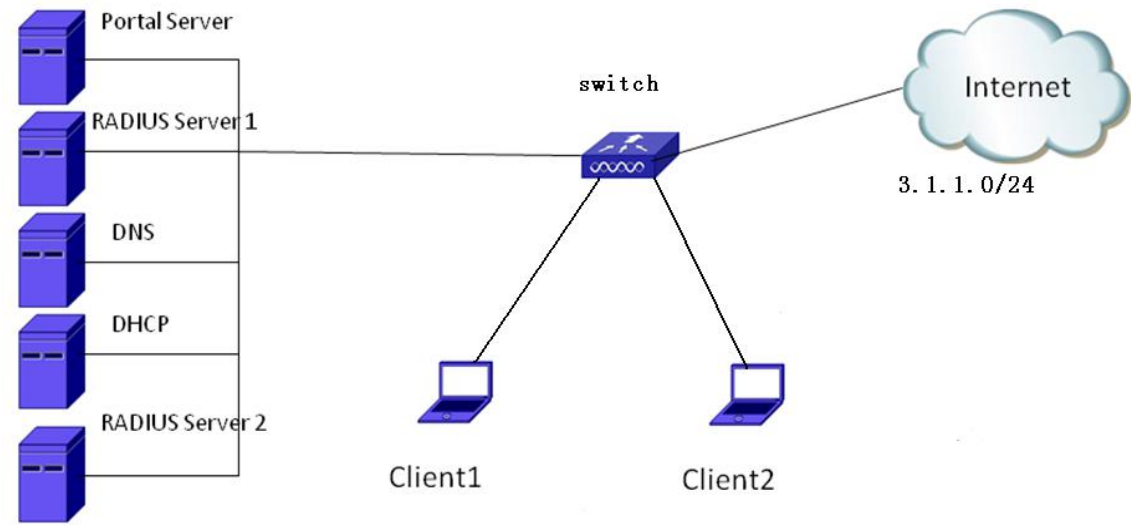


图 13-4 认证白名单功能配置图

配置步骤：

为 pc1 和 pc2 配置免 portal 认证白功能

Switch1 (config)#free-mac 68-74-7f-29-76-04 ff-ff-ff-ff-ff

Switch1 (config)#free-mac 00-03-0f-11-11-11 ff-ff-ff-ff-ff

13.4.4 认证白名单功能排错帮助

- 当在使用认证白名单过程中遇到问题，请检查是否是如下原因：
- ☞ 配置的 free mac 是否和 client 的 mac 相匹配；
 - ☞ Client 和交换机互连的端口是否开启了 portal 规则。

13.5 认证成功页面自动推送（暂不支持）

13.5.1 认证成功页面自动推送介绍

认证成功后页面自动推送功能就是在用户通过认证后，能够重新打开用户所需要访问的

网页。根据实际情况可以配置用户认证成功后自动推送认证前访问页面，或者自动推送指定的网页。

13.5.2 认证成功后页面自动推送配置

认证成功后页面自动推送功能配置序列：

- 1. 打开或关闭 captive portal 认证功能
- 2. 配置认证成功后页面自动推送功能

1. 打开或关闭 captive portal 认证功能

命令	解释
Captive portal 配置模式	
enable	全局打开或关闭交换机的 captive portal 功能。
disable	

2. 配置认证成功后页面自动推送功能

命令	解释
Captive portal instance 配置模式	
redirect attribute url-after-login enable no redirect attribute url-after-login enable	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。
redirect attribute url-after-login name <name> no redirect attribute url-after-login name	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。
redirect attribute url-after-login encode {plain-text base64}	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。
redirect attribute url-after-login value <url-value> no redirect attribute url-after-login value	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。

13.5.3 认证成功后页面自动推送举例

案例：

在 configuration 1 中配置认证成功后页面自动推送功能，认证成功后自动推送页面 http://www.test.com。

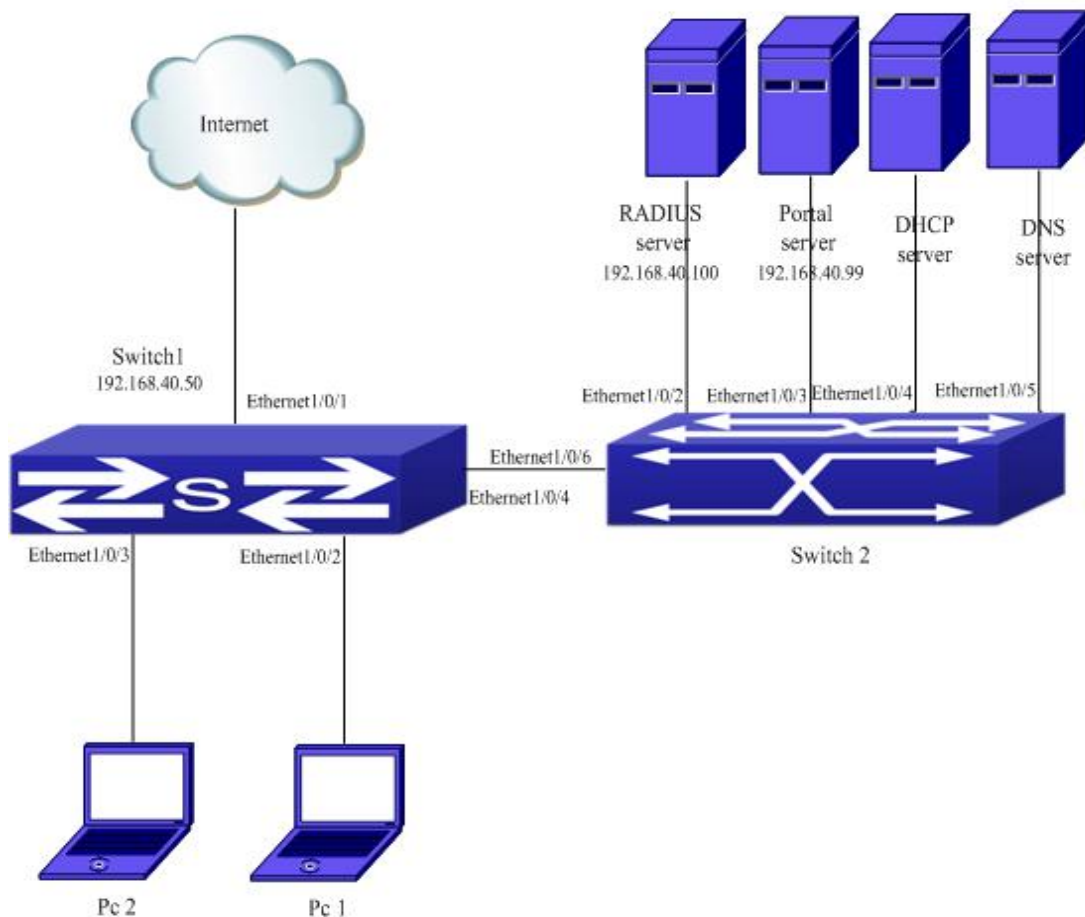


图 13-5 认证成功后页面自动推送功能配置

配置步骤：

为 siwitch1 配置 portal 服务器信息

```
switch1 (config-cp)#enable
```

```
switch1 (config-cp)#configuration 1
```

```
switch1 (config-cp-instance)#enable
```

```
switch1 (config-cp-instance)# redirect attribute url-after-login enable
```

```
switch1 (config-cp-instance)# redirect attribute url-after-login encode plain-text
```

```
switch1 (config-cp-instance)# redirect attribute url-after-login name ad
```

```
switch1 (config-cp-instance)# redirect attribute url-after-login value http://www.test.com
```

13.5.4 认证成功后页面自动推送排错帮助

当在使用认证成功后页面自动推送功能过程中遇到问题，请检查是否是如下原因：

- ☞ 是否正确配置了 **captive portal** 的认证功能。认证成功后页面自动推送功能需要 **captive portal** 功能正常的情况下才能生效。
- ☞ 若配置了命令 **redirect attribute url-after-login value**，则认证通过后页面自动推送配置的页面地址，若没有配置该命令则推送的页面为用户认证前访问的页面。
- ☞ 客户端认证前访问的页面或命令指定的推送页面是否存在，若不存在页面推送后也无法

访问。

13.6 http-redirect-filter

13.6.1 http-redirect-filter 介绍

http-redirect-filter 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。

此功能与 Captive Portal 功能结合使用，即在开启了 Captive Portal 接入认证的情况下，实现对用户的访问进行过滤。

13.6.2 http-redirect-filter 配置

http-redirect-filter 功能配置序列：

- 1. 配置 http-redirect-filter 规则
- 2. 配置 http-redirect-filter 规则到 cp instance 中

1. 配置 http-redirect-filter 规则

命令	解释
captive portal 模式	
http-redirect-filter <1-32> (ip A.B.C.D domain WORD) no http-redirect-filter (<1-32> all)	配置 http-redirect-filter 规则。本命令的 no 形式为删除规则。

2. 配置 http-redirect-filter 规则到 cp instance 中

命令	解释
captive portal 模式	
http-redirect-filter <1-32> no http-redirect-filter (<1-32> all)	绑定 http-redirect-filter 规则到 captive portal configuration 下。本命令的 no 形式为解除 captive portal configuration 下 http-redirect-filter 的绑定。

13.6.3 http-redirect-filter 举例

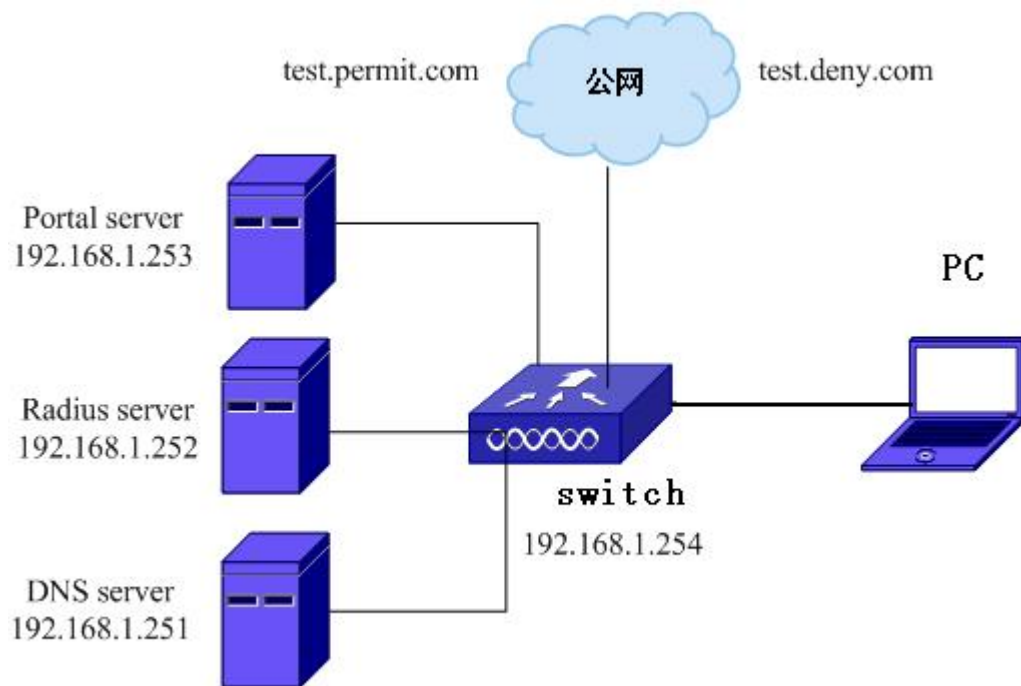


图 13-6 http-redirect-filter 功能典型案例

如上图所示的拓扑，client 在通过 portal 认证前想要访问公网地址“test.permit.com”需要配置 url 白名单，client 认证通过后需要禁止访问公网地址“test.deny.com”需要配置 url 黑名单。

按照以下步骤进行配置：

1. 全局模式下配置 RADIUS server 相关的认证密钥，认证服务器，计费服务器，aaa 模式等信息：

```
switch (config)#radius-server key 0 test
switch (config)#radius-server authentication host 192.168.1.252
switch (config)#radius-server accounting host 192.168.1.252
switch (config)#aaa-accounting enable
switch (config)#aaa enable
switch (config)#aaa group server radius radius_aaa_1
switch config-sg-radius)# server 192.168.1.252
switch(config)#interface vlan 192
switch(config-if-vlan1)#ip address 192.16.1.254 255.255.255.0
switch(config)#free-resource 1 destination ipv4 192.168.1.252/32
```

2. portal 实例下 Portal 功能、配置 Portal Server 服务器等信息：

```
Switch (config)#captive-portal
Switch (config-cp)#enable
Switch(config-cp)# nas-ipv4 192.168.1.254
Switch(config-cp)# external portal-server server-name abc ipv4 192.168.1.253
```

```
Switch (config-cp)# configuration 1
Switch (config-cp-instance)#enable
Switch (config-cp-instance)#name helix4
Switch (config-cp-instance)#radius accounting
Switch (config-cp-instance)#radius-acct-server abc99
Switch (config-cp-instance)#radius-auth-server abc99
Switch (config-cp-instance)#redirect attribute nas-ip enable
Switch (config-cp-instance)#ac-name helix4
Switch (config-cp-instance)#redirect url-head http://192.168.1.253/a70.htm
Switch (config-cp-instance)#portal-server ipv4 abc
```

3. 配置 http-redirect-filter 规则:

```
Switch (config)#captive-portal
Switch (config-cp)# http-redirect-filter 1 domain test.permit.com
Switch (config-cp)#configuration 1
Switch (config-cp-instance)# http-redirect-filter 1
```

4. 端口上开启 portal 功能:

```
Switch (config)# interface ethernet1/0/2
Switch (config-if-ethernet1/0/2)#portal enable configuration 1
```

通过配置，可以看出在 client 认证通过前只有访问“test.permit.com”，才能正常重定向认证，访问其它地址，则不能重定向。

13.6.4 http-redirect-filter 排错帮助

在使用中，如果发现 http-redirect-filter 功能无法正常使用，可以采用下面的检查步骤：

- ☞ 查看配置的匹配的规则内容是否与访问的域名匹配；
- ☞ DNS server 的配置是否正确，能否正确解析出配置的域名；
- ☞ captive-portal configuration 下 http-redirect-filter 命令是否配置。

13.7 Portal 无感知

13.7.1 Portal 无感知介绍

MAC 认证具备“一次认证，多次使用”用户体验。如果开通了 MAC 快速认证，用户首次登陆 Portal 页面成功认证后，后续用户就可以用任意应用上网。

为了实现大量用户的 MAC 快速认证，必须使用外置的服务器来保存 MAC 绑定信息，并且能够动态的添加，而不是手动添加，这一新的实现方案被称为 MAC 快速认证方案，

由于用户再次接入网络时不需要手动输入用户名和密码进行认证，因此也称为 Portal 无感知认证方案。

13.7.2 Portal 无感知配置

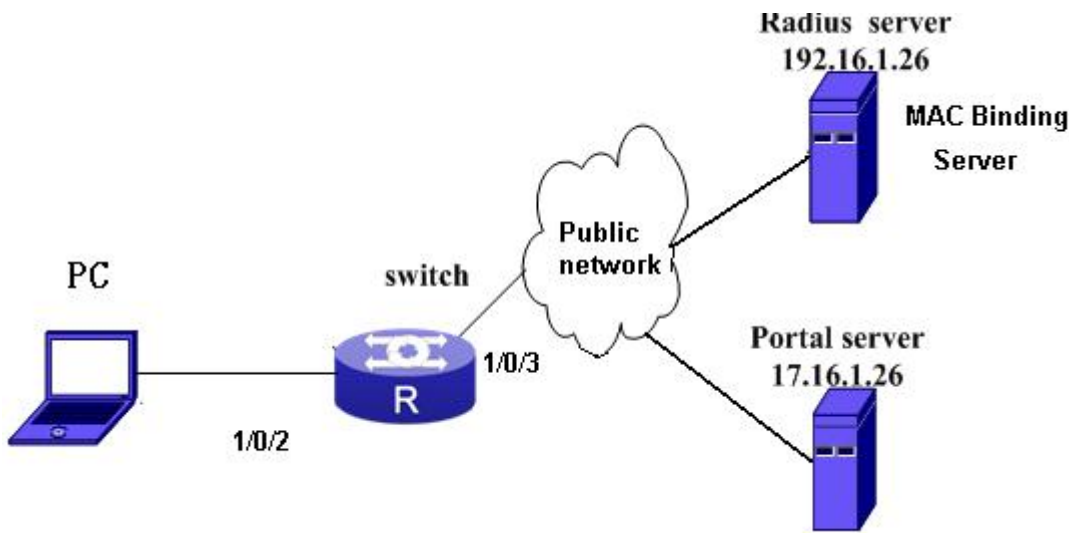
1. 开启/关闭 mac 快速认证功能

命令	解释
captive portal config 模式	
fast-mac-auth	开启或关闭 mac 快速认证功能。
no fast-mac-auth	

13.7.3 Portal 无感知举例

搭建环境如下图所示，其中包括以下几部分：

- 1、PC，用户通过交换机接入网络。
- 2、公共网，此部分可以没有，也可以是其他的交换机设备。
- 3、服务器，其中包括：
MAC 绑定服务器，用于保存曾经认证通过的终端 MAC 地址；
Radius 服务器，用于对用户进行 portal 认证和计费；
Portal 服务器，用于对用户进行 portal 认证时使用；
MAC 绑定服务器、Radius 服务器、portal 服务器可以是一台设备，MAC 绑定服务器是在 Radius 服务器上的扩展。



按照以下步骤进行配置：

- 1. 具体的配置如下：全局模式下配置 RADIUS server 相关的认证密钥，认证服务器，计费服务器，aaa 模式等信息：
switch (config)#radius-server key 0 test
switch (config)#radius-server authentication host 192.16.1.26
switch (config)#radius-server accounting host 192.16.1.26
switch (config)#aaa-accounting enable

```
switch (config)#aaa enable
switch (config)#aaa group server radius radius_aaa_1
switch (config-sg-radius)# server 192.16.1.26
switch (config)#interface vlan 192
switch (config-if-vlan1)#ip address 192.16.1.50 255.255.255.0
switch (config)#free-resource 1 destination ipv4 192.16.1.26/32
```

2. portal 实例下 Portal 功能、配置 Portal Server 服务器等信息：

```
Switch (config)#captive-portal
Switch (config-cp)#enable
Switch (config-cp)# nas-ipv4 192.168.1.50
Switch (config-cp)# external portal-server server-name abc ipv4 172.16.1.26
Switch (config-cp)# configuration 1
Switch (config-cp-instance)#enable
Switch (config-cp-instance)#name helix4
Switch (config-cp-instance)#radius accounting
Switch (config-cp-instance)#radius-acct-server abc99
Switch (config-cp-instance)#radius-auth-server abc99
Switch (config-cp-instance)#redirect attribute nas-ip enable
Switch (config-cp-instance)#ac-name helix4
Switch (config-cp-instance)#redirect url-head http://172.16.1.26/a70.htm
Switch (config-cp-instance) # portal-server ipv4 abc
```

3. 配置 portal 无感知：

```
Switch (config-cp)#enable
Switch (config-cp)#fast-mac-auth
```

4. 端口上开启 portal 功能：

```
Switch (config)# interface ethernet1/0/2
Switch (config-if-ethernet1/0/2)#portal enable configuration 1
```

用户第一次访问网络需要 portal 正常认证，之后即可以 portal 无感知认证。

13.7.4 Portal 无感知排错帮助

使用 Portal 无感知功能过程中如遇到问题，请检查是否是以下原因导致：

- ☞ 查看是否已开启 captive-portal 功能；
- ☞ 查看是否已开启 mac 快速认证功能；
- ☞ 配置完成 mac 快速认证功能后如果未生效查看是否向交换机下发了 app 表项。

13.8 Portal 逃生

在目前的 Portal 实际组网应用中，存在这样一个风险，当接入设备与 Portal 服务器的通信中断，会造成新用户无法上线，已经在线的 Portal 用户无法正常下线，接入设备和 Portal 服务器信息不一致引起的计费错误。这些现象会给网络运营商和使用者带来很大的不便。

针对上面的问题，portal 逃生功能提供了一个很好的解决方式，在 Portal 服务器或者 radius 服务器无法正常工作的前提下，让已经在线用户仍然可以正常使用网络，新用户仍然可以上线接入网络，因此 Portal 逃生又分 portal server 逃生和 radius server 逃生。

13.8.1 Portal Server 逃生功能

13.8.1.1 Portal Server 逃生介绍

Portal server 逃生功能的原理：交换机周期性探测 Portal 服务器，若探测成功则将服务器状态置为 UP，若探测失败 N 次（N 可配置）则将不可达则变成 Down 状态（逃生状态），取消网络的认证限制，允许 Portal 用户不需经过认证即可访问网络资源，并发送状态改变的 Trap 信息和日志。当探测到服务器可达时，恢复服务器状态为 Up 状态（认证状态），并重新开启网络认证限制，不允许未认证的用户访问网络，并发送状态恢复的日志和 Trap。

交换机探测 Portal 服务器状态的具体实现方式是探测 TCP 连接：交换机定期向 Portal 服务器的 portal 服务端口（默认 2000，可配置）发起 TCP 连接。若连接成功建立则表示此服务器的 portal 服务已开启，就认为一次探测成功且服务器可达（状态为 Up）；若连接失败则认为一次探测失败。

探测周期及最大探测失败次数：通过命令行可以配置每次探测之间的时间间隔，此间隔称为探测周期。最大探测失败次数是判断服务器不可达前所必须经历的连续探测失败次数。一次探测失败并不一定认为服务器不可达，而需要查看连续探测失败的次数是否达到配置的最大探测失败次数，若达到此值则认为服务器不可达，否则只是累加，当某次探测成功后，此值会自动清零。探测周期及最大探测失败次数都可以通过命令进行配置。

服务器从可达状态变为不可达状态时触发如下三个操作，管理员可以通过配置选择：

- 发送 Trap：向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal 服务器名以及该服务器状态改变前后的状态等信息。
- 发送日志：向日志服务器发送日志信息。日志信息中记录了 Portal 服务器名以及该服务器状态改变前后的状态等信息。
- 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。

服务器从不可达状态变为可达状态时触发如下三个操作，其中发送 Trap 和发送日志可通过配置选择，关闭 Portal 逃生是系统强制执行的：

- 发送 Trap：向网管服务器发送 Trap 信息。Trap 信息中记录了 Portal 服务器名

以及该服务器状态改变前后的状态等信息。

- 发送日志：向日志服务器发送日志信息。日志信息中记录了 Portal 服务器名以及该服务器状态改变前后的状态等信息。
- 关闭 Portal 逃生：Portal 服务器变为可达（up）时，恢复该 VAP 的 Portal 认证功能，新上线的用户必须通过 Portal 认证后才能访问网络资源。

注意：Portal 逃生目前只能实现新旧用户访问网络不受影响，至于用户无法正常下线，目前提供其他方式进行处理，如若 portal server 恢复 UP，接入设备将用户强制下线，保证用户下线处理正常。

13.8.1.2 Portal Server 逃生基本配置

Portal 逃生功能的基本配置序列：

1. 打开 Portal 逃生功能，并配置探测周期和最大失败次数。
2. 显示 Portal 服务器的当前连接状态。

1. 打开 Portal 逃生功能，并配置探测周期和最大失败次数

命令	解释
Captive Portal 全局配置模式	
portal-server-detect server-name <name> [interval <interval>] [retry <retries>][action {log permit-all trap }] no portal-server-detect server-name <name>	开启 Portal 逃生功能，并配置（可选）探测周期、最大失败次数和服务器状态发生变化时的操作。该命令的 NO 命令关闭 Portal 逃生功能。

2. 显示 Portal 服务器的当前连接状态

命令	解释
特权模式	
show captive-portal ext-portal-server server-name <name> status	显示 Portal 逃生服务器的状态。

13.8.1.3 Portal Server 逃生配置举例

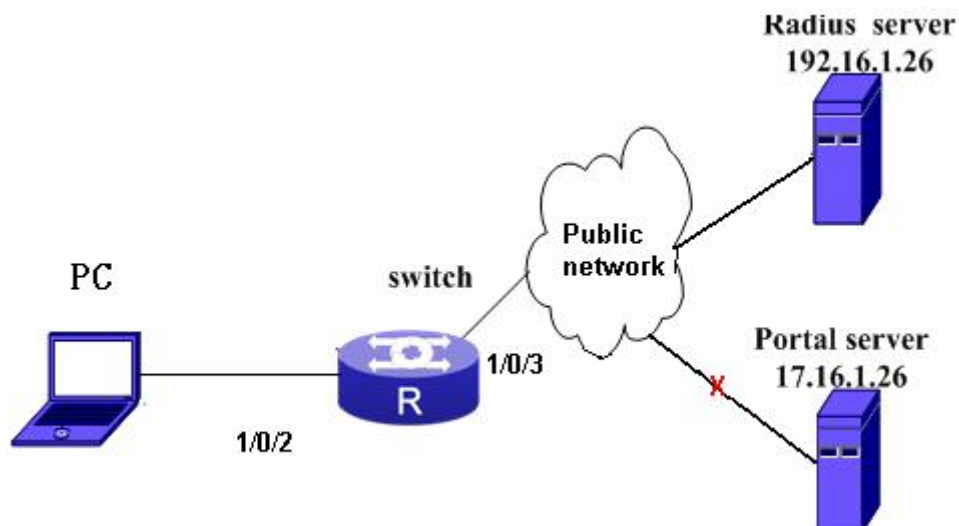


图 13-7 Portal Server 逃生功能典型案例

如上图所示的拓扑，在 Portal server 正常可达的情况下，客户端上线时可以进行正常的 Portal 认证后接入网络。当 portal server 由于本身宕机或者和交换机间的链路断开时，如果交换机没有开启 Portal 逃生功能，客户端将无法认证上线。如果交换机开启 Portal 逃生功能，交换机就能探测到 Portal server 已经不可用，就会启动 Portal 逃生，客户端不需要认证就可以访问网络。如果客户端在 Portal server 断开前就已经通过认证，也不会受到影响，仍然可以访问网络。

具体的配置如下：

1. 全局模式下配置 RADIUS server 相关的认证密钥，认证服务器，计费服务器，aaa 模式等信息：

```
switch (config)#radius-server key 0 test
switch (config)#radius-server authentication host 192.16.1.26
switch (config)#radius-server accounting host 192.16.1.26
switch (config)#aaa-accounting enable
switch (config)#aaa enable
switch (config)#aaa group server radius radius_aaa_1
switch config-sg-radius)# server 192.16.1.26
switch(config)#interface vlan 192
switch(config-if-vlan1)#ip address 192.16.1.50 255.255.255.0
switch(config)#free-resource 1 destination ipv4 192.16.1.26/32
```

2. portal 实例下 Portal 功能、配置 Portal Server 服务器等信息：

```
Switch (config)#captive-portal
Switch (config-cp)#enable
Switch(config-cp)# nas-ipv4 192.168.1.50
Switch(config-cp)# external portal-server server-name abc ipv4 172.16.1.26
Switch (config-cp)# configuration 1
```

```
Switch (config-cp-instance)#enable
Switch (config-cp-instance)#name helix4
Switch (config-cp-instance)#radius accounting
Switch (config-cp-instance)#radius-acct-server abc99
Switch (config-cp-instance)#radius-auth-server abc99
Switch (config-cp-instance)#redirect attribute nas-ip enable
Switch (config-cp-instance)#ac-name helix4
Switch (config-cp-instance)#redirect url-head http://172.16.1.26/a70.htm
Switch (config-cp-instance) # portal-server ipv4 abc
```

3. 配置 portal 逃生:

```
Switch (config-cp)#enable
Switch (config-cp)# portal-server-detect server-name abc interval 600 retry 2 action log
permit-all trap
```

4. 端口上开启 portal 功能:

```
Switch (config)# interface ethernet1/0/2
Switch (config-if-ethernet1/0/2)#portal enable configuration 1
```

以上过程, Portal 服务器 abc 绑定到 CP instance, 配置了对该服务器的探测功能, 每次探测间隔时间为 600 秒, 若连续二次探测均失败, 则发送服务器不可达的 Trap 信息和日志信息, 并打开 Portal 逃生功能, 允许未认证用户访问网络。

13.8.1.4 Portal Server 逃生排错帮助

在使用中, 如果发现 Portal 逃生功能不能生效, 可以采用下面的检查步骤:

- ☞ `show captive-portal ext-portal-server server-name <name> status` 检查 Portal server 的 Detect Mode 是否为 enable, 如果没有 enable, 说明没有开启该 Portal server 的逃生功能, 需要开启。
- ☞ 如果 Portal 逃生功能已经开启, 检查 Detect Operational Status 的状态是否为 down, 只有在服务器状态为 down 时, 逃生功能才会启动。
- ☞ 如果 Portal 服务器的状态已经为 down, 逃生功能仍然不生效, 可能是设备出现了问题, 需要联系售后工程师处理。

13.8.2 Radius Server 逃生功能

13.8.2.1 Radius Server 逃生介绍

打开 radius server 逃生功能以后, 当所有的 radius 认证服务器不可达时, 逃生功能生效, 此时 portal 认证客户端的流量放行。当探测到某个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。

13.8.2.2 Radius Server 逃生基本配置

Radius server 逃生功能的基本配置序列：

- 1. 打开 radius server 逃生功能
- 2. 配置对 radius server 进行可达性探测的周期

1. 打开 radius 逃生功能

命令	解释
全局配置模式	
radius-server escape {enable disable }	开启 radius server 逃生功能。

2. 配置对 radius server 进行可达性探测的周期

命令	解释
全局配置模式	
radius-server escape detection-interval {default <second>}	配置对 radius server 进行可达性探测的周期，默认为 180s。

13.8.2.3 Radius Server 逃生配置举例

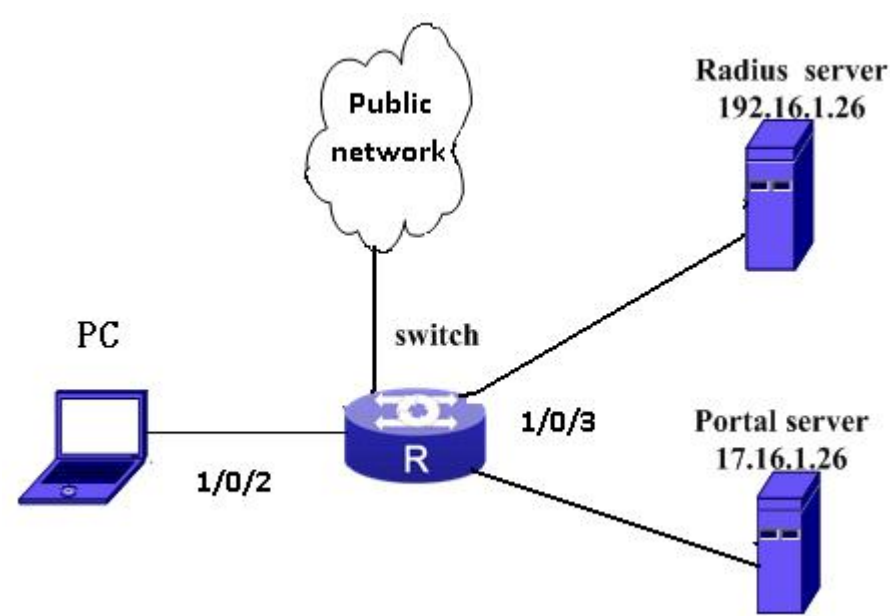


图 13-8 Radius server 逃生功能典型案例

- 具体的配置如下：
- 1 全局模式下配置 RADIUS server 相关的认证密钥，认证服务器，计费服务器，aaa 模式等信息：

```
switch (config)#radius-server key 0 test
switch (config)#radius-server authentication host 192.16.1.26
switch (config)#radius-server accounting host 192.16.1.26
switch (config)#aaa-accounting enable
switch (config)#aaa enable
switch (config)#aaa group server radius radius_aaa_1
switch config-sg-radius)# server 192.16.1.26
switch(config)#interface vlan 192
switch(config-if-vlan1)#ip address 192.16.1.50 255.255.255.0
switch(config)#free-resource 1 destination ipv4 192.16.1.26/32
```

2 portal 实例下 Portal 功能、配置 Portal Server 服务器等信息：

```
Switch (config)#captive-portal
Switch (config-cp)#enable
Switch(config-cp)# nas-ipv4 192.168.1.50
Switch(config-cp)# external portal-server server-name abc ipv4 172.16.1.26
Switch (config-cp)# configuration 1
Switch (config-cp-instance)#enable
Switch (config-cp-instance)#name helix4
Switch (config-cp-instance)#radius accounting
Switch (config-cp-instance)#radius-acct-server abc99
Switch (config-cp-instance)#radius-auth-server abc99
Switch (config-cp-instance)#redirect attribute nas-ip enable
Switch (config-cp-instance)#ac-name helix4
Switch (config-cp-instance)#redirect url-head http://172.16.1.26/a70.htm
Switch (config-cp-instance) # portal-server ipv4 abc
```

3 配置 radius server 逃生：

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

4 端口上开启 portal 功能：

```
Switch (config)# interface ethernet1/0/2
Switch (config-if-ethernet1/0/2)#portal enable configuration 1
```

以上过程每隔 120s 则对 radius server 进行周期性的可达性探测。

13.8.2.4 Radius Server 逃生排错帮助

在使用中，如果发现 radius server 逃生功能不生效，可以采用下面的检查步骤：

- ☞ 检查是否开启了 radius server 逃生功能；
- ☞ 如果开启了该功能，通过 `show aaa config` 获得 Retransmit 和 Time Out 这两项参数值，然后检查配置的 `detection-interval` 是否大于 $(\text{Retransmit}+1)*\text{Time Out}$ 所获得的值，如果小于，则逃生失败；
- ☞ 如果 `show aaa config` 显示 `Is Server live by radius escape function =0` 说明逃生中，但是功能不生效，则需要联系售后工程师处理。