目 录

1 端口安全配置

1.1 端口安全简介

1.1.1 概述

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。这里的非法报文是指：

- MAC 地址未被端口学习到的用户报文；
- 未通过认证的用户报文。

说明

由于端口安全特性通过多种安全模式提供了 802.1X 和 MAC 地址认证的扩展和组合应用，因此在需要灵活使用以上两种认证方式的组网环境下，推荐使用端口安全特性。关于 802.1X、MAC 地址认证特性的详细介绍和具体配置请参见“安全配置指导”中的“802.1X”、“MAC 地址认证”。

1.1.2 端口安全的特性

1. Need To Know特性（NTK）

Need To Know 特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证或被端口学习到的 MAC 所属的设备或主机上，从而防止非法设备窃听网络数据。

2. 入侵检测（Intrusion Protection）特性

入侵检测特性指通过检测从端口收到的数据帧的源 MAC 地址，对接收非法报文的端口采取相应的安全策略，包括端口被暂时断开连接、永久断开连接或 MAC 地址被过滤（默认 3 分钟，不可配），以保证端口的安全性。

3. Trap特性

Trap 特性是指当端口有特定的数据包（由非法入侵，用户上下线等原因引起）传送时，设备将会发送 Trap 信息，便于网络管理员对这些特殊的行为进行监控。

1.1.3 端口安全模式

基本的端口安全模式可大致分为两大类：控制 MAC 学习类和认证类。

- 控制 MAC 学习类无需认证，包括端口自动学习 MAC 地址和禁止 MAC 地址学习两种模式。
- 认证类利用 MAC 地址认证和 802.1X 认证机制来实现，包括单独认证和组合认证等多种模式。

配置了安全模式的端口上收到用户报文后，首先查找MAC地址表，如果该报文的源MAC地址已经存在于MAC地址表中，则端口转发该报文，否则根据端口所在安全模式进行相应的处理（学习、认证），并在发现非法报文后触发端口执行相应的安全防护措施（Need To Know、入侵检测）或发送Trap告警。关于各模式的具体工作机制，以及是否触发Need To Know、入侵检测的具体情况请参见 表 1-1。

表1-1 端口安全模式描述表

安全模式		工作机制	NTK/入侵检测
缺省情况	noRestrictions	表示端口的安全功能关闭，端口处于无限制状态	无效
端口控制MAC 地址学习	autoLearn	端口可通过手工配置或自动学习 MAC 地址。这些新的 MAC 地址被称为安全 MAC，并被添加到安全 MAC 地址表中 当端口下的安全MAC地址数超过端口允许学习的最大安全MAC地址数后，端口模式会自动转变为 secure 模式。之后，该端口停止添加新的安全 MAC，只有源 MAC 地址为安全 MAC 地址、手工配置的 MAC 地址的报文，才能通过该端口 该模式下，端口禁止学习动态 MAC 地址	可触发
	secure	禁止端口学习MAC地址，只有源MAC地址为端口上的安全MAC地址、手工配置的 MAC 地址的报文，才能通过该端口	
端口采用802.1X 认证	userLogin	对接入用户采用基于端口的 802.1X 认证 此模式下，端口下的第一个 802.1X 用户认证成功后，其它用户无须认证就可接入	无效
	userLoginSecure	对接入用户采用基于 MAC 地址的 802.1X 认证 此模式下，端口最多只允许一个 802.1X 认证用户接入	可触发
	userLoginWithOUI	该模式与 userLoginSecure 模式类似，但端口上除了允许一个 802.1X 认证用户接入之外，还额外允许一个特殊用户接入，该用户报文的源 MAC 的 OUI 与设备上配置的 OUI 值相符 在用户接入方式为有线的情况下，802.1X 报文进行 802.1X 认证，非 802.1X 报文直接进行 OUI 匹配，802.1X 认证成功和 OUI 匹配成功的报文都允许通过端口	
	userLoginSecureExt	对接入用户采用基于 MAC 的 802.1X 认证，且允许端口下有多个 802.1X 用户	
端口采用MAC 地址认证	macAddressWithRadius	对接入用户采用 MAC 地址认证 此模式下，端口允许多个用户接入	可触发

安全模式		工作机制	NTK/入侵检测
端口采用802.1X和MAC地址认证组合认证	macAddressOrUserLoginSecure	端口同时处于userLoginSecure模式和macAddressWithRadius模式 在用户接入方式为有线的情况下，非802.1X报文直接进行MAC地址认证，802.1X报文直接进行802.1X认证	可触发
	macAddressElseUserLoginSecure	端口同时处于macAddressWithRadius模式和userLoginSecure模式，但MAC地址认证优先级大于802.1X认证； 非802.1X报文直接进行MAC地址认证。802.1X报文先进行MAC地址认证，如果MAC地址认证失败再进行802.1X认证	
	macAddressOrUserLoginSecureExt	与macAddressOrUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户	
	macAddressElseUserLoginSecureExt	与macAddressElseUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户	

说明

- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全MAC地址数与相应模式下允许认证用户数的最小值。例如，userLoginSecureExt模式下，端口下所允许的最大用户为配置的最大安全MAC地址数与802.1X认证所允许的最大用户数的最小值。
- 手工配置MAC地址的具体介绍请参见“二层技术-以太网交换命令参考”中的“MAC地址表”。

窍门

由于安全模式种类较多，为便于记忆，部分端口安全模式名称的构成可按如下规则理解:

- “userLogin”表示基于端口的802.1X认证;
- “macAddress”表示MAC地址认证;
- “Else”之前的认证方式先被采用，失败后根据请求认证的报文协议类型决定是否转为“Else”之后的认证方式。
- “Or”连接的两种认证方式无固定生效顺序，设备根据请求认证的报文协议类型决定认证方式.
- 携带“Secure”的userLogin表示基于MAC地址的802.1X认证。
- 携带“Ext”表示可允许多个802.1X用户认证成功，不携带则表示仅允许一个802.1X用户认证成功。

1.1.4 端口安全对Guest VLAN和Auth-Fail VLAN的支持

802.1X认证的Guest VLAN是指允许用户在未认证的情况下，可以访问的指定VLAN。802.1X的Auth-Fail VLAN与MAC地址认证的Guest VLAN是指允许用户在认证失败的情况下，可以访问的指定VLAN。

- 对于支持 802.1X 认证的安全模式来说，可配置基于 MAC 地址的 Guest VLAN 和基于 MAC 地址的 Auth-Fail VLAN，分别简称为 MGV 和 MAFV。关于 802.1X 认证的 MGV 和 MAFV 的具体介绍请参见“安全配置指导”中的“802.1X”。
- 对于支持 MAC 地址认证的安全模式来说，可配置 Guest VLAN。关于 MAC 地址认证 Guest VLAN 的具体介绍请参见“安全配置指导”中的“MAC 地址认证”。

说明

若端口上同时配置了 802.1X 认证的 MAFV(MAC-based Auth-Fail VLAN)与 MAC 地址认证的 Guest VLAN，则后生成的 MAFV 表项会覆盖先生成的 Guest VLAN 表项，但后生成的 Guest VLAN 表项不能覆盖先生成的 MAFV 表项。

1.2 端口安全配置任务简介

表1-2 端口安全配置任务简介

配置任务		说明	详细配置
使能端口安全功能		必选	1.3
配置端口允许的最大安全 MAC 地址数		可选	1.4
配置端口安全模式		必选	1.5
配置端口安全的特性	配置 Need To Know 特性	可选 根据实际组网需求选择其中一种或多种特性	1.6
	配置入侵检测特性		
	配置 Trap 特性		
配置安全 MAC 地址		可选	1.7
配置当前端口不应用服务器下发的授权信息		可选	1.8

1.3 使能端口安全功能

1.3.1 配置准备

在使能端口安全功能之前，需要关闭全局的 802.1X 和 MAC 地址认证功能。

1.3.2 使能端口安全功能

表1-3 使能端口安全功能

操作	命令	说明
进入系统视图	**system-view**	-
使能端口安全功能	**port-security enable**	必选 缺省情况下，未使能端口安全功能

注意

端口安全功能使能后，端口的如下配置会被自动恢复为括弧内的缺省情况:

- 802.1X 认证（关闭）、端口接入控制方式（**macbased**）、端口接入控制模式（**auto**）；
- MAC 地址认证（关闭）。

且以上配置不能再进行手动配置，只能随端口安全模式的改变由系统配置。

端口安全功能关闭时，端口的如下配置会被自动恢复为（括弧内的）缺省情况:

- 端口安全模式（noRestrictions）；
- 802.1X 认证（关闭）、端口接入控制方式（**macbased**）、端口接入控制模式（**auto**）；
- MAC 地址认证（关闭）。

端口上有用户在线的情况下，端口安全功能无法关闭。

说明

- 有关 802.1X 认证配置的详细介绍可参见“安全配置指导”中的“802.1X”。
- 有关 MAC 地址认证配置的详细介绍可参见“安全配置指导”中的“MAC 地址认证”。

1.4 配置端口允许的最大安全MAC地址数

端口安全允许某个端口下有多个用户通过认证，但是允许的用户数不能超过规定的最大值。

配置端口允许的最大安全 MAC 地址数有两个作用：

- 控制能够通过某端口接入网络的最大用户数；
- 控制端口安全能够添加的安全 MAC 地址数。

表1-4 配置端口允许的最大安全 MAC 地址数

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置端口允许的最大安全 MAC 地址数	**port-security max-mac-count** *count-value*	必选 缺省情况下，最大安全 MAC 地址数不受限制

说明

- 本特性仅在 SAP 板工作在二层模式时支持。
- 该配置与“二层技术-以太网交换配置指导/MAC 地址表”中配置的端口最多可以学习到的 MAC 地址数无关。

1.5 配置端口安全模式

1.5.1 配置准备

在配置端口安全模式之前，端口上需要满足以下条件：

- 802.1X 认证关闭、端口接入控制方式为 **macbased**、端口接入控制模式为 **auto**；
- MAC 地址认证关闭。

（如果以上条件不满足，则系统会提示错误信息，且不能进行端口安全模式的配置；如果端口上已经配置了端口安全模式，则以上配置就不允许改变。）

- 对于 autoLearn 模式，还需要提前设置端口允许的最大安全 MAC 地址数。

说明

- 在端口安全功能未使能的情况下，端口安全模式可以进行配置但不会生效。
- 端口上有用户在线的情况下，端口安全模式无法改变。

1.5.2 配置端口安全模式

表1-5 配置端口安全安全模式

操作	命令	说明
进入系统视图	**system-view**	-
配置允许通过认证的用户 OUI 值	**port-security oui** *oui-value* **index** *index-value*	可选 缺省情况下，没有配置允许通过认证的用户 OUI 值 该命令仅在配置 **userlogin-withoui** 安全模式时必选
进入接口视图	**interface** *interface-type interface-number*	- -autoLearn 模式只能在二层以太网类型的接口下配置 - userloginWithOUI 模式只能在二层以太网接口下配置

操作	命令	说明
配置端口的安全模式	**port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure | userlogin | userlogin-secure | userlogin-secure-ext | userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }**	必选 缺省情况下，端口处于 noRestrictions 模式

说明

- 本特性仅在 SAP 板工作在二层模式时支持。
- 当端口工作于 autoLearn 模式时，无法更改端口允许的最大安全 MAC 地址数。
- OUI（Organizationally Unique Identifier）是 MAC 地址的前 24 位（二进制），是 IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符。
- 允许通过认证的用户 OUI 值可以配置多个，但在端口安全模式为 userLoginWithOUI 时，端口除了可以允许一个 802.1X 的接入用户通过认证之外，仅允许其中一个 OUI 值所属的用户通过认证。
- 当端口安全已经使能且当前端口安全模式不是 noRestrictions 时，若要改变端口安全模式，必须首先执行 **undo port-security port-mode** 命令恢复端口安全模式为 noRestrictions 模式。

1.6 配置端口安全的特性

1.6.1 配置Need To Know特性

该功能用来限制认证端口上出方向的报文转发。即，用户通过认证后，以此 MAC 为目的地址的报文都可以正常转发。可以设置以下三种方式：

- **ntkonly**：仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过。
- **ntk-withbroadcasts**：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过。
- **ntk-withmulticasts**：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过。

配置了 Need To Know 的端口在以上任何一种方式下都不允许目的 MAC 地址未知的单播报文通过。

表1-6 配置 Need To Know 特性

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置端口 Need To Know 特性	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }	必选 缺省情况下，端口没有配置 Need To Know 特性，即所有报文都可成功发送

说明

本特性仅在 SAP 板工作在二层模式时支持。

1.6.2 配置入侵检测特性

当设备检测到一个非法的用户通过端口试图访问网络时，该特性用于配置设备可能对其采取的安全措施，包括以下三种方式：

- **blockmac**：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中，源 MAC 地址为阻塞 MAC 地址的报文将被丢弃。此 MAC 地址在被阻塞 3 分钟（系统默认，不可配）后恢复正常。
- **disableport**：表示将收到非法报文的端口永久关闭。
- **disableport-temporarily**：表示将收到非法报文的端口暂时关闭一段时间。关闭时长可通过 **port-security timer disableport** 命令配置。

表1-7 配置入侵检测特性

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置入侵检测特性	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	必选 缺省情况下，不进行入侵检测处理
退回系统视图	**quit**	-
配置系统暂时关闭端口连接的时间	**port-security timer disableport** *time-value*	可选 缺省情况下，系统暂时关闭端口连接的时间为 20 秒

说明

- 本特性仅在 SAP 板工作在二层模式时支持。
- macAddressElseUserLoginSecure 或 macAddressElseUserLoginSecureExt 安全模式下工作的端口，对于同一个报文，只有 MAC 地址认证和 802.1X 认证均失败后，才会触发入侵检测特性。

1.6.3 配置Trap特性

该特性用于端口上发生关键事件时触发告警开关输出对应的 Trap 信息，包括以下几种情况：

- **addresslearned**：端口学习到新 MAC 地址时发出告警信息。
- **dot1xlogfailure/dot1xlogon/dot1xlogoff**：802.1X 用户认证失败/认证成功/下线时发出告警日志。
- **ralmlogfailure/ralmlogon/ralmlogoff**：MAC 地址认证用户认证失败/认证成功/下线时发出告警信息。
- **intrusion**：发现非法报文时发出告警信息。

表1-8 配置 Trap 特性

操作	命令	说明
进入系统视图	**system-view**	-
打开指定告警信息的开关	**port-security trap { addresslearned | dot1xlogfailure | dot1xlogoff | dot1xlogon | intrusion | ralmlogfailure | ralmlogoff | ralmlogon }**	必选 缺省情况下，所有告警信息的开关处于关闭状态

1.7 配置安全MAC地址

安全 MAC 地址是一种特殊的 MAC 地址，不会被老化，保存后重启设备，不会丢失。在同一个 VLAN 内，一个安全 MAC 地址只能被添加到一个端口上，利用该特点，可以实现同一 VLAN 内 MAC 地址与端口的绑定。

安全 MAC 地址可以通过以下两种途径生成：

- 由 autoLearn 安全模式下的使能端口安全功能的端口自动学习
- 通过命令行或者 MIB 手动配置

当端口下的安全 MAC 地址数目超过端口允许学习的最大安全 MAC 地址数后，该端口不会再添加新的安全 MAC 地址，仅接收并允许数据帧中的源 MAC 地址为安全 MAC 地址的报文访问网络设备。

1.7.1 配置准备

在配置安全 MAC 地址之前，需要完成以下任务：

- 使能端口安全功能
- 设置端口允许的最大安全 MAC 地址数
- 配置端口安全模式为 autoLearn

1.7.2 配置安全MAC地址

表1-9 配置安全 MAC 地址

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
配置安全 MAC 地址	在系统视图下	**port-security mac-address security** *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	二者必选其一 缺省情况下，未配置安全 MAC 地址
	在接口视图下	**interface** *interface-type interface-number*	
		port-security mac-address security *mac-address* **vlan** *vlan-id*	

说明

配置的安全 MAC 地址会被写入配置文件，端口 up 或 down 时不会丢失。保存配置文件后，即使设备重启，安全 MAC 地址也不会被删除。

1.8 配置当前端口不应用服务器下发的授权信息

802.1X 用户或 MAC 地址认证用户在 RADIUS 服务器上通过认证时，服务器会把授权信息下发给设备端。通过此配置可实现基于端口是否忽略 RADIUS 服务器下发的授权信息。

表1-10 配置当前端口不应用服务器下发的授权信息

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置当前端口不应用 RADIUS 服务器下发的授权信息	**port-security authorization ignore**	必选 缺省情况下，端口应用 RADIUS 服务器下发的授权信息

说明

本特性仅在 SAP 板工作在二层模式时支持。

1.9 端口安全显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后端口安全的运行情况，通过查看显示信息验证配置的效果。

表1-11 端口安全显示和维护

操作	命令
显示端口安全的配置信息、运行情况和统计信息	**display port-security** [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

操作	命令
显示安全 MAC 地址信息	**display port-security mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示阻塞 MAC 地址信息	**display port-security mac-address block** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.10 端口安全典型配置举例

1.10.1 端口安全autoLearn模式配置举例

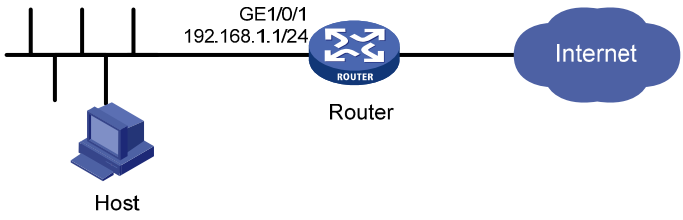
1. 组网需求

在 Router 的端口 GigabitEthernet1/0/1 上对接入用户做如下的限制：

- 允许 64 个用户自由接入，不进行认证，将学习到的用户 MAC 地址添加为安全 MAC 地址；
- 当安全 MAC 地址数量达到 64 后，停止学习；当再有新的 MAC 地址接入时，触发入侵检测，并将此端口关闭 30 秒。

2. 组网图

图1-1 端口安全 autoLearn 模式组网图



3. 配置步骤

(1) 具体的配置步骤

```
<Router> system-view
```

使能端口安全功能。

```
[Router] port-security enable
```

打开入侵检测 Trap 开关。

```
[Router] port-security trap intrusion
[Router] interface gigabitethernet 1/0/1
```

设置端口允许的最大安全 MAC 地址数为 64。

```
[Router-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 autoLearn。

```
[Router-GigabitEthernet1/0/1] port-security port-mode autolearn
```

设置触发入侵检测特性后的保护动作为暂时关闭端口，关闭时间为 30 秒。

```
[Router-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Router-GigabitEthernet1/0/1] quit
[Router] port-security timer disableport 30
```

(2) 验证配置结果

上述配置完成后，可以用 **display** 命令显示端口安全配置情况，如下：

```
[Router] display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Intrusion trap is enabled
 Disableport Timeout: 30s
 OUI value:

GigabitEthernet1/0/1 is link-up
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is DisablePortTemporarily
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
```

可以看到端口的最大安全 MAC 数为 64，端口模式为 autoLearn，入侵检测 Trap 开关打开，入侵保护动作为 DisablePortTemporarily，入侵发生后端口禁用时间为 30 秒。

配置完成后，允许地址学习，学习到的 MAC 地址数可以用上述命令显示，如学习到 5 个，那么存储的安全 MAC 地址数就为 5，可以在接口视图下用 **display this** 命令查看学习到的 MAC 地址，如：

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security 0002-0000-0015 vlan 1
 port-security mac-address security 0002-0000-0014 vlan 1
 port-security mac-address security 0002-0000-0013 vlan 1
 port-security mac-address security 0002-0000-0012 vlan 1
 port-security mac-address security 0002-0000-0011 vlan 1
#
```

当学习到的 MAC 地址数达到 64 后，用命令 **display port-security interface** 可以看到端口模式变为 secure，再有新的 MAC 地址到达将触发入侵保护，Trap 信息如下：

```
#Jul 14 10:39:47:135 2009 Router PORTSEC/4/VIOLATION:Traph3cSecureViolation
 An intrusion occurs!
 IfIndex: 9437185
 Port: 9437185
 MAC Addr: 00:02:00:00:00:32
 VLAN ID: 1
 IfAdminStatus: 1
```

并且可以通过下述命令看到端口安全将此端口关闭：

```
[Router-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state:  Port Security Disabled
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface
 ......
```

30 秒后，端口状态恢复：

```
[Router-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface
 ......
```

此时，如手动删除几条安全 MAC 地址后，端口安全的状态重新恢复为 autoLearn，可以继续学习 MAC 地址。

1.10.2 端口安全userLoginWithOUI模式配置举例

1. 组网需求

客户端通过端口 GigabitEthernet1/0/1 连接到 Router 上，Router 通过 RADIUS 服务器对客户端进行身份认证，如果认证成功，客户端被授权允许访问 Internet 资源。

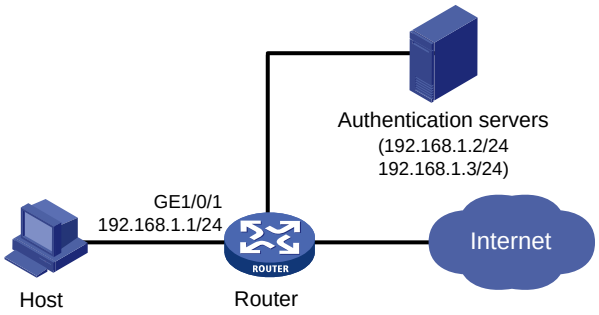
- IP 地址为 192.168.1.2 的 RADIUS 服务器作为主认证/备份计费服务器，IP 地址为 192.168.1.3 的 RADIUS 服务器作为备份认证/主计费服务器。认证共享密钥为 name，计费共享密钥为 money。
- 所有接入用户都使用 ISP 域 sun 的缺省认证/授权/计费方案，该域最多可容纳 30 个用户；
- 系统向 RADIUS 服务器重发报文的时间间隔为 5 秒，重发次数为 5 次，发送实时计费报文的时间间隔为 15 分钟，发送的用户名不带域名。

Router 的管理者希望对接入用户的端口 GigabitEthernet1/0/1 做如下限制：

- 允许一个 802.1X 用户上线；
- 最多可以配置 16 个 OUI 值，还允许端口上有一个与 OUI 值匹配的 MAC 地址用户通过。

2. 组网图

图1-2 端口安全 userLoginWithOUI 模式组网图



3. 配置步骤

说明

- 下述配置步骤包含了部分 AAA/RADIUS 协议配置命令，具体介绍请参见“安全配置指导”中的“AAA”。
- 客户端和 RADIUS 服务器之间路由可达，认证相关的配置略。

(1) 具体的配置步骤

- 配置 RADIUS 协议

```
<Router> system-view
```

配置 RADIUS 方案。

```
[Router] radius scheme radsun
[Router-radius-radsun] primary authentication 192.168.1.2
[Router-radius-radsun] primary accounting 192.168.1.3
[Router-radius-radsun] secondary authentication 192.168.1.3
[Router-radius-radsun] secondary accounting 192.168.1.2
[Router-radius-radsun] key authentication name
[Router-radius-radsun] key accounting money
[Router-radius-radsun] timer response-timeout 5
[Router-radius-radsun] retry 5
[Router-radius-radsun] timer realtime-accounting 15
[Router-radius-radsun] user-name-format without-domain
[Router-radius-radsun] quit
```

配置 ISP 域。

```
[Router] domain sun
[Router-isp-sun] authentication default radius-scheme radsun
[Router-isp-sun] authorization default radius-scheme radsun
[Router-isp-sun] accounting default radius-scheme radsun
[Router-isp-sun] access-limit enable 30
[Router-isp-sun] quit
```

- 配置 802.1X

配置 802.1X 的认证方式为 CHAP。（该配置可选，缺省情况下 802.1X 的认证方式为 CHAP）

```
[Router] dot1x authentication-method chap
```

- 配置端口安全特性

使能端口安全功能。

```
[Router] port-security enable
```

添加 5 个 OUI 值。

```
[Router] port-security oui 1234-0100-1111 index 1
[Router] port-security oui 1234-0200-1111 index 2
[Router] port-security oui 1234-0300-1111 index 3
[Router] port-security oui 1234-0400-1111 index 4
[Router] port-security oui 1234-0500-1111 index 5
[Router] interface gigabitethernet 1/0/1
```

设置端口安全模式为 userLoginWithOUI。

```
[Router-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
[Router-GigabitEthernet1/0/1] quit
```

(2) 验证配置结果

查看名为 radsun 的 RADIUS 方案的配置信息：

```
[Router] display radius scheme radsun
SchemeName  : radsun
  Index : 1                           Type : standard
  Primary Auth Server:
```

```
    IP: 192.168.1.2                           Port: 1812   State: active
    Encryption Key : N/A
    VPN instance   : N/A
  Primary Acct Server:
    IP: 192.168.1.3                           Port: 1813   State: active
    Encryption Key : N/A
    VPN instance   : N/A
  Second Auth Server:
    IP: 192.168.1.3                           Port: 1812   State: active
    Encryption Key : N/A
    VPN instance   : N/A
  Second Acct Server:
    IP: 192.168.1.2                           Port: 1813   State: active
    Encryption Key : N/A
    VPN instance   : N/A
  Auth Server Encryption Key : name
  Acct Server Encryption Key : money
  Accounting-On packet disable, send times : 5 , interval : 3s
  Interval for timeout(second)                              : 5
  Retransmission times for timeout                          : 5
  Interval for realtime accounting(minute)                  : 15
  Retransmission times of realtime-accounting packet        : 5
  Retransmission times of stop-accounting packet            : 500
  Quiet-interval(min)                                       : 5
  Username format                                           : without-domain
  Data flow unit                                            : Byte
  Packet unit                                               : one
```

查看名为 sun 的 ISP 域的配置信息：

```
[Router] display domain sun
   Domain : sun
   State : Active
   Access-limit : 30
   Accounting method : Required
   Default authentication scheme      : radius:radsun
   Default authorization scheme       : radius:radsun
   Default accounting scheme          : radius:radsun
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes:
```

查看端口安全的配置信息：

```
[Router] display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 123401
   Index is 2,  OUI value is 123402
```

```
  Index is 3,  OUI value is 123403
  Index is 4,  OUI value is 123404
  Index is 5,  OUI value is 123405

 GigabitEthernet1/0/1 is link-up
  Port mode is userLoginWithOUI
  NeedToKnow mode is disabled
  Intrusion Protection mode is NoAction
  Max MAC address number is not configured
  Stored MAC address number is 0
  Authorization is permitted
```

配置完成后，如果有 802.1X 用户上线，则可以看到存储的安全 MAC 地址数为 1。还可以通过下述命令查看 802.1X 用户的情况：

```
[Router] display dot1x interface GigabitEthernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD quick deploy is disabled

  Configuration: Transmit Period   30 s,  Handshake Period       15 s
                 Quiet Period      60 s,  Quiet Period Timer is disabled
                 Supp Timeout      30 s,  Server Timeout        100 s
                 Reauth Period   3600 s
                 The maximal retransmitting times    2
  EAD quick deploy configuration:
               EAD timeout:    30m

 The maximum 802.1X user resource number is 2048 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-up
  802.1X protocol is enabled
  Proxy trap checker is   disabled
  Proxy logoff checker is disabled
  Handshake is enabled
  Handshake secure is disabled
  802.1X unicast-trigger is enabled
  Periodic reauthentication is disabled
  The port is an authenticator
  Authentication Mode is Auto
  Port Control Type is Mac-based
  802.1X Multicast-trigger is enabled
  Mandatory authentication domain: NOT configured
  Guest VLAN: NOT configured
  Auth-Fail VLAN: NOT configured
  Max number of on-line users is 1024
```

```
   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
        EAP Success Packets: 4, Fail Packets: 5
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

   Controlled User(s) amount to 1
```

此外，端口还允许一个与 OUI 值匹配的 MAC 地址的用户通过，可以通过下述命令查看：

```
[Router] display mac-address interface GigabitEthernet 1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX               AGING TIME(s)
1234-0300-0011  1         Learned        GigabitEthernet1/0/1     AGING

  ---  1 mac address(es) found  ---
```

1.10.3 端口安全macAddressElseUserLoginSecure模式配置举例

1. 组网需求

客户端通过端口 GigabitEthernet1/0/1 连接到 Router 上，Router 通过 RADIUS 服务器对客户端进行身份认证。如果认证成功，客户端被授权允许访问 Internet 资源。

Router 的管理者希望对接入用户的端口 GigabitEthernet1/0/1 做如下的限制：

- 可以有多个 MAC 认证用户上线；
- 如果是 802.1X 用户请求认证，先进行 MAC 地址认证，MAC 地址认证失败，再进行 802.1X 认证。802.1X 用户限制为 1 个；
- MAC 地址认证设置用户名格式为自定义用户名和密码的形式，上线的 MAC 地址认证用户和 802.1X 认证用户总和不能超过 64 个；
- 为防止报文发往未知目的 MAC 地址，启动 Need To Know 特性。

2. 组网图

同 图 1-2所示。

3. 配置步骤

说明

- RADIUS认证/计费及ISP域的配置同 1.10.2 ，这里不再赘述。
- 接入用户和 RADIUS 服务器之间路由可达，认证相关的配置略。

---

(1) 具体的配置步骤

```
<Router> system-view
```

使能端口安全功能。

```
[Router] port-security enable
```

配置 MAC 认证的用户名为 aaa，密码为 123456。

```
[Router] mac-authentication user-name-format fixed account aaa password simple 123456
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Router] mac-authentication domain sun
[Router] interface gigabitethernet 1/0/1
```

配置 802.1X 的认证方式为 CHAP。（该配置可选，缺省情况下 802.1X 的认证方式为 CHAP）

```
[Router] dot1x authentication-method chap
```

设置端口允许的最大安全 MAC 地址数为 64。

```
[Router-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 macAddressElseUserLoginSecure。

```
[Router-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

设置端口 Need To Know 模式为 ntkonly。

```
[Router-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
[Router-GigabitEthernet1/0/1] quit
```

(2) 验证配置结果

查看端口安全的配置信息：

```
[Router] display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 Disableport Timeout: 20s
 OUI value:

 GigabitEthernet1/0/1 is link-up
   Port mode is macAddressElseUserLoginSecure
   NeedToKnow mode is NeedToKnowOnly
   Intrusion Protection mode is NoAction
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
```

查看 MAC 地址认证情况：

```
[Router] display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
 User name format is fixed account
 Fixed username:aaa
 Fixed password:123456
          Offline detect period is 60s
          Quiet period is 5s
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 3
          Current domain is mac

Silent MAC User info:
          MAC Addr         From Port                    Port Index
```

```
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 3, failed: 7
 Max number of on-line users is 256
  Current online user number is 3
    MAC ADDR         Authenticate state           Auth Index
    1234-0300-0011   MAC_AUTHENTICATOR_SUCCESS     13
    1234-0300-0012   MAC_AUTHENTICATOR_SUCCESS     14
    1234-0300-0013   MAC_AUTHENTICATOR_SUCCESS     15
```

查看 802.1X 认证情况：

```
<Router> display dot1x interface GigabitEthernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled
 EAD quick deploy is disabled

 Configuration: Transmit Period   30 s,  Handshake Period       15 s
                Quiet Period      60 s,  Quiet Period Timer is disabled
                Supp Timeout      30 s,  Server Timeout        100 s
                The maximal retransmitting times    2
 EAD quick deploy configuration:
                EAD timeout:    30m

 Total maximum 802.1X user resource number is 2048 per slot
 Total current used 802.1X resource number is 1

 GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Proxy trap checker is   disabled
   Proxy logoff checker is disabled
   Handshake is enabled
   Handshake secure is disabled
   802.1X unicast-trigger is enabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   802.1X Multicast-trigger is enabled
   Mandatory authentication domain: NOT configured
   Guest VLAN: NOT configured
   Auth-Fail VLAN: NOT configured
   Max number of on-line users is 1024

   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
```

```
        EAP Success Packets: 4, Fail Packets: 5
  Received EAPOL Start Packets : 6
           EAPOL LogOff Packets: 2
           EAP Response/Identity Packets : 80
           EAP Response/Challenge Packets: 6
           Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

   Controlled User(s) amount to 1
```

此外，因为设置了 Need To Know 特性，目的 MAC 地址未知、广播和多播报文都被丢弃。

1.11 常见配置错误举例

1.11.1 端口安全模式无法设置

1. 故障现象

无法配置端口安全模式。

```
[Router-GigabitEthernet1/0/1] port-security port-mode autolearn
 Error:When we change port-mode, we should first change it to noRestrictions, then change
it to the other.
```

2. 故障分析

在当前端口安全模式已配置的情况下，无法直接对端口安全模式进行设置。

3. 处理过程

首先设置端口安全模式为 noRestrictions 状态。

```
[Router-GigabitEthernet1/0/1] undo port-security port-mode
[Router-GigabitEthernet1/0/1] port-security port-mode autolearn
```

1.11.2 无法配置端口安全MAC地址

1. 故障现象

无法配置端口安全 MAC 地址。

```
[Router-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
 Error: Security MAC address configuration failed.
Error:Can not operate security MAC address for current port mode is not autoLearn!
```

2. 故障分析

端口安全模式为非 autoLearn 时，不能对安全 MAC 地址进行设置。

3. 处理过程

设置端口安全模式为 autoLearn 状态。

```
[Router-GigabitEthernet1/0/1] undo port-security port-mode
[Router-GigabitEthernet1/0/1] port-security max-mac-count 64
[Router-GigabitEthernet1/0/1] port-security port-mode autolearn
[Router-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

1.11.3 用户在线情况下无法更换端口安全模式

1. 故障现象

802.1X 或 MAC 地址认证用户在线的情况下，更换端口安全模式失败。

```
[Router-GigabitEthernet1/0/1] undo port-security port-mode
 Error:Cannot configure port-security for there is 802.1X user(s) on line on port GigabitEthernet1/0/1.
```

2. 故障分析

有 802.1X 或 MAC 认证用户在线的情况下，禁止更换端口安全模式。

3. 处理过程

断开端口与用户的连接后再进行端口安全模式更换，可以通过 **cut** 命令强制切断连接。

```
[Router-GigabitEthernet1/0/1] quit
[Router] cut connection interface gigabitethernet 1/0/1
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] undo port-security port-mode
```