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。而在仅需要 802.1X、MAC 地址认证特性来完成接入控制的组网环境下，推荐单独使用以上两个特性。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. 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。

2. 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地址数超过端口安全允许学习的最大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，其他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
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； 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，取端口安全所允许的最大 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端口安全所允许的最大 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 Guest VLAN 和 Auth-Fail VLAN。关于 802.1X 认证的 Guest VLAN 和 Auth-Fail VLAN 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 Auth-Fail VLAN 与 MAC 地址认证的 Guest VLAN，则后生成的 Auth-Fail VLAN 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 Auth-Fail VLAN 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
配置端口安全允许的最大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	配置入侵检测特性	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，端口安全功能处于关闭状态

注意

执行使能或关闭端口安全功能的命令后，端口上的如下配置会被自动恢复为以下缺省情况:

- 802.1X 端口接入控制方式为 **macbased**、802.1X 端口的授权状态为 **auto**。
- 端口安全模式为 noRestrictions。

当端口安全功能处于使能状态时，端口上的 802.1X 功能以及 MAC 地址认证功能将不能被手动开启，且 802.1X 端口接入控制方式和端口接入控制模式也不能被修改，只能随端口安全模式的改变由系统更改。

在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 配置端口安全允许的最大MAC地址数

端口安全允许某个端口下有多个用户接入，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 MAC 地址数有两个作用：

- 控制端口允许接入网络的最大用户数。最终端口上允许接入的用户数为此处配置的最大 MAC 地址数和相应认证类安全模式下允许的用户数的较小值；
- 控制 autoLearn 模式下端口能够添加的最大安全 MAC 地址数。

表1-4 配置端口安全允许的最大 MAC 地址数

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置端口安全允许的最大MAC地址数	**port-security max-mac-count** *count-value*	必选 缺省情况下，最大MAC地址数不受限制

说明

端口安全允许的最大 MAC 地址数与“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，且不受其影响。

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。
- MAC 地址认证关闭。
- 端口未加入聚合组。

（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安全允许的最大 MAC 地址数。但是如果端口已经工作在 autoLearn 模式下，则无法更改端口安全允许的最大 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
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
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

- 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1-6 配置入侵检测特性

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**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

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。

1.6.2 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1-7 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，不会因为端口状态的变化而被丢失。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。
- 通过命令行手动添加。

缺省情况下，所有的安全 MAC 地址均不老化，除非被管理员通过命令行手工删除，或因为配置的改变（端口的安全模式被改变，或端口安全功能被关闭）而被系统自动删除。但是，安全 MAC 地址不老化会带来一些问题，比如合法用户离开端口后，若有非法用户仿冒合法用户源 MAC 接入，会导致合法用户不能继续接入；或者虽然该合法用户已离开，但仍然占用端口 MAC 地址资源，而导致其他合法用户不能接入。因此，让某一类安全 MAC 地址能够定期老化，可提高端口接入的安全性和端口资源的利用率。我们将这类可老化的安全 MAC 地址称为 Sticky MAC。

表1-8 安全 MAC 地址相关属性列表

生成方式	是否可老化	配置保存机制	老化机制
手工添加（未指定**sticky**关键字）	不老化，称之为静态类型的安全MAC地址	安全MAC地址在保存配置文件并重启设备后，仍然存在	无
手工添加（指定**sticky**关键字） 端口自动学习	可老化（老化时间可配），称之为Sticky MAC地址 • 若老化时间为 0，则表示不老化（缺省） • 若老化时间不为 0，则表示安全 MAC 地址会老化 Sticky MAC地址可通过配置转换为动态类型的MAC地址	• Sticky MAC 地址在保存配置文件并重启设备后，仍然存在，且其老化定时器会重新开始计时（缺省） • 动态类型的安全 MAC 地址不能被保存在配置文件中，设备重启后会被丢失	• 定时老化（缺省） • 无流量老化 说明：无论是Sticky MAC地址还是动态类型的安全MAC地址，均遵循此老化机制

说明

- 动态类型的安全 MAC 地址与 Sticky MAC 地址可通过配置相互转换，两者本质相同，仅配置保存方式不同。
- 无流量老化方式下，设备会定期检测（检测周期不可配）端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的 Sticky MAC 地址老化时间内没有任何流量产生，则才会被老化。
- 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 地址的报文和源 MAC 地址为手工配置的 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，需要完成以下配置任务：

- 使能端口安全功能
- 设置端口安全允许的最大 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**	-
配置安全MAC地址的老化时间		**port-security timer autolearn aging** *time-value*	可选 缺省情况下，安全MAC地址不会老化
配置安全MAC地址	在系统视图下	**port-security mac-address security** [**sticky**] *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
	在二层以太网端口视图下	**interface** *interface-type interface-number*	
		port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*	
		quit	
进入二层以太网端口视图		**interface** *interface-type interface-number*	-
配置安全地址的老化方式为无流量老化		**port-security mac-address aging-type inactivity**	可选 缺省情况下，安全MAC地址按照固定时间进行老化，即在配置的安全MAC地址的老化时间到达后立即老化

操作	命令	说明
将Sticky MAC地址设置为动态类型的安全MAC地址	**port-security mac-address dynamic**	可选 缺省情况下，Sticky MAC地址能够被保存在配置文件中，设备重启后也不会丢失

说明

- 无流量老化方式下，设备会定期检测（检测周期固定，不可配）端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的安全 MAC 地址老化时间内没有任何流量产生，则才会被老化。
- 动态类型的安全 MAC 地址不会被保存在配置文件中，可通过执行 **display port-security mac-address security** 命令查看到，设备重启之后会丢失。

1.8 配置当前端口不应用下发的授权信息

802.1X 用户或 MAC 地址认证用户在 RADIUS 服务器或设备上通过认证时，服务器或设备会把授权信息下发给用户。通过此配置可实现基于端口是否忽略 RADIUS 服务器或设备本地下发的授权信息。

表1-10 配置当前端口不应用下发的授权信息

操作	命令	说明
进入系统视图	**system-view**	-
进入二层以太网端口视图	**interface** *interface-type interface-number*	-
配置当前端口不应用RADIUS服务器或设备本地下发的授权信息	**port-security authorization ignore**	必选 缺省情况下，端口应用RADIUS服务器或设备本地下发的授权信息

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*]
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*]

操作	命令
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

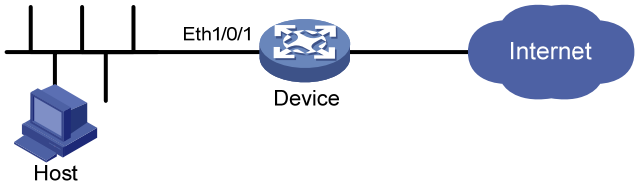
1. 组网需求

在 Device 的端口 Eth1/0/1 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 Sticky 安全 MAC 地址，老化时间为 30 分钟；
- 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

```
<Device> system-view
```

使能端口安全功能。

```
[Device] port-security enable
```

设置 Sticky MAC 地址的老化时间为 30 分钟。

```
[Device] port-security timer autolearn aging 30
```

打开入侵检测 Trap 开关。

```
[Device] port-security trap intrusion
[Device] interface ethernet 1/0/1
```

设置端口安全允许的最大 MAC 地址数为 64。

```
[Device-Ethernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 autoLearn。

```
[Device-Ethernet1/0/1] 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。

```
[Device-Ethernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-Ethernet1/0/1] quit
[Device] 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：

```
[Device] display port-security interface ethernet 1/0/1
 Equipment port-security is enabled
 Intrusion trap is enabled
 AutoLearn aging time is 30 minutes
 Disableport Timeout: 30s
 OUI value:

Ethernet1/0/1 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
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

可以看到端口安全所允许的最大 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，可以在端口视图下用 **display this** 命令查看学习到的 MAC 地址，如：

```
[Device] interface ethernet 1/0/1
[Device-Ethernet1/0/1] display this
#
interface Ethernet1/0/1
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security sticky 0002-0000-0015 vlan 1
 port-security mac-address security sticky 0002-0000-0014 vlan 1
 port-security mac-address security sticky 0002-0000-0013 vlan 1
 port-security mac-address security sticky 0002-0000-0012 vlan 1
 port-security mac-address security sticky 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：

```
#Jan 14 10:39:47:135 2011 Device PORTSEC/4/VIOLATION: Trap1.3.6.1.4.1.25506.2.26.1.
3.2<hh3cSecureViolation>:
 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：

```
[Device-Ethernet1/0/1] display interface ethernet 1/0/1
```

```
 Ethernet1/0/1 current state: DOWN (  Port Security Disabled  )
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: Ethernet1/0/1 Interface
 ......
```

30 秒后，端口状态恢复：

```
[Device-Ethernet1/0/1] display interface ethernet 1/0/1
 Ethernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: Ethernet1/0/1 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 Eth1/0/1 连接到 Device 上，Device 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。

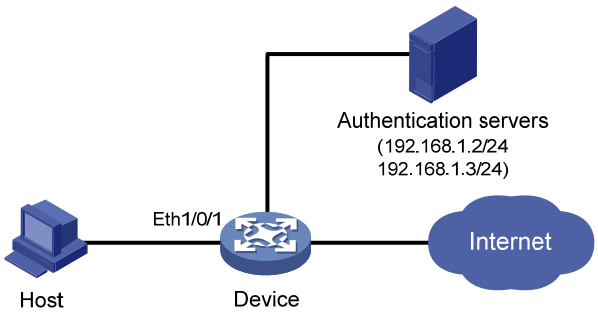
- IP 地址为 192.168.1.2 的 RADIUS 服务器作为主认证/备份计费服务器，IP 地址为 192.168.1.3 的 RADIUS 服务器作为备份认证/主计费服务器。认证共享密钥为 name，计费共享密钥为 money。
- 所有接入用户都使用 ISP 域 sun 的缺省认证/授权/计费方案，该域最多可容纳 30 个用户；
- 系统向 RADIUS 服务器重发报文的时间间隔为 5 秒，重发次数为 5 次，发送实时计费报文的时间间隔为 15 分钟，发送的用户名不带域名。

Device 的管理者希望对接入用户的端口 Eth1/0/1 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

```
<Device> system-view
```

配置 RADIUS 方案。

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

配置 ISP 域。

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

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

- 配置端口安全特性

使能端口安全功能。

```
[Device] port-security enable
```

添加 5 个 OUI 值。

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

设置端口安全模式为 userLoginWithOUI。

```
[Device-Ethernet1/0/1] port-security port-mode userlogin-withoui
[Device-Ethernet1/0/1] quit
```

(2) 验证配置结果

查看名为 radsun 的 RADIUS 方案的配置信息：

```
[Device] 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
    Probe username : N/A
    Probe interval : N/A
  Primary Acct Server:
    IP: 192.168.1.3                             Port: 1813   State: active
    Encryption Key : N/A
  Second Auth Server:
    IP: 192.168.1.3                             Port: 1812   State: active
    Encryption Key : N/A
    Probe username : N/A
    Probe interval : N/A
  Second Acct Server:
    IP: 192.168.1.2                             Port: 1813   State: active
    Encryption Key : N/A
  Auth Server Encryption Key : ******
  Acct Server Encryption Key : ******
  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：

```
[Device] 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：

```
[Device] display port-security interface ethernet 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

 Ethernet1/0/1 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
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

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：

```
[Device] display dot1x interface ethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 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 1024 per slot
 Total current used 802.1X resource number is 1

 Ethernet1/0/1  is link-up
   802.1X protocol is enabled
   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
   Critical VLAN: NOT configured
   Critical recovery-action: NOT configured
   Max number of on-line users is 256

   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：

```
[Device] display mac-address interface ethernet 1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX                      AGING TIME(s)
1234-0300-0011  1         Learned        Ethernet1/0/1                   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 Eth1/0/1 连接到 Device 上，Device 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。

Device 的管理者希望对接入用户的端口 Eth1/0/1 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 地址认证用户使用 MAC 地址作为用户名和密码，其中 MAC 地址带连字符、字母小写；
- 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。

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

```
<Device> system-view
```

使能端口安全功能。

```
[Device] port-security enable
```

配置 MAC 地址的认证方式为 PAP。（该配置可选，缺省情况下 MAC 地址的认证方式为 PAP）

```
[Device] mac-authentication authentication-method pap
```

配置 MAC 地址认证用户名格式：使用带连字符的 MAC 地址作为用户名与密码，其中字母小写。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Device] mac-authentication domain sun
```

```
[Device] interface ethernet 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）

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

设置端口安全允许的最大 MAC 地址数为 64。

```
[Device-Ethernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 macAddressElseUserLoginSecure。

```
[Device-Ethernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

(2) 验证配置结果

查看端口安全的配置信息：

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

 Ethernet1/0/1 is link-up
   Port mode is macAddressElseUserLoginSecure
   Intrusion Protection mode is NoAction
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

查看 MAC 地址认证情况：

```
[Device] display mac-authentication interface ethernet 1/0/1
MAC address authentication is enabled.
 PAP authentication is enabled
```

```
 User name format is MAC address in lowercase,like xx-xx-xx-xx-xx-xx
 Fixed username: mac
 Fixed password: not configured
          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

Ethernet1/0/1 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：

```
<Device> display dot1x interface ethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 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 1024 per slot
 Total current used 802.1X resource number is 1

 Ethernet1/0/1  is link-up
   802.1X protocol is enabled
   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
  Critical VLAN: NOT configured
  Critical recovery-action: NOT configured
  Max number of on-line users is 256

  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
```

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。

```
[Device-Ethernet1/0/1] 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。

```
[Device-Ethernet1/0/1] undo port-security port-mode
[Device-Ethernet1/0/1] 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。

```
[Device-Ethernet1/0/1] port-security mac-address security 1-1-2 vlan 1
 Error: Security MAC address configuration failed.
```

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。

```
[Device-Ethernet1/0/1] undo port-security port-mode
[Device-Ethernet1/0/1] port-security max-mac-count 64
[Device-Ethernet1/0/1] port-security port-mode autolearn
[Device-Ethernet1/0/1] 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。

```
[Device-Ethernet1/0/1] undo port-security port-mode
 Error:Cannot configure port-security for there is 802.1X user(s) on line on port
Ethernet1/0/1.
```

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。

```
[Device-Ethernet1/0/1] quit
[Device] cut connection interface ethernet 1/0/1
[Device] interface ethernet 1/0/1
[Device-Ethernet1/0/1] undo port-security port-mode
```