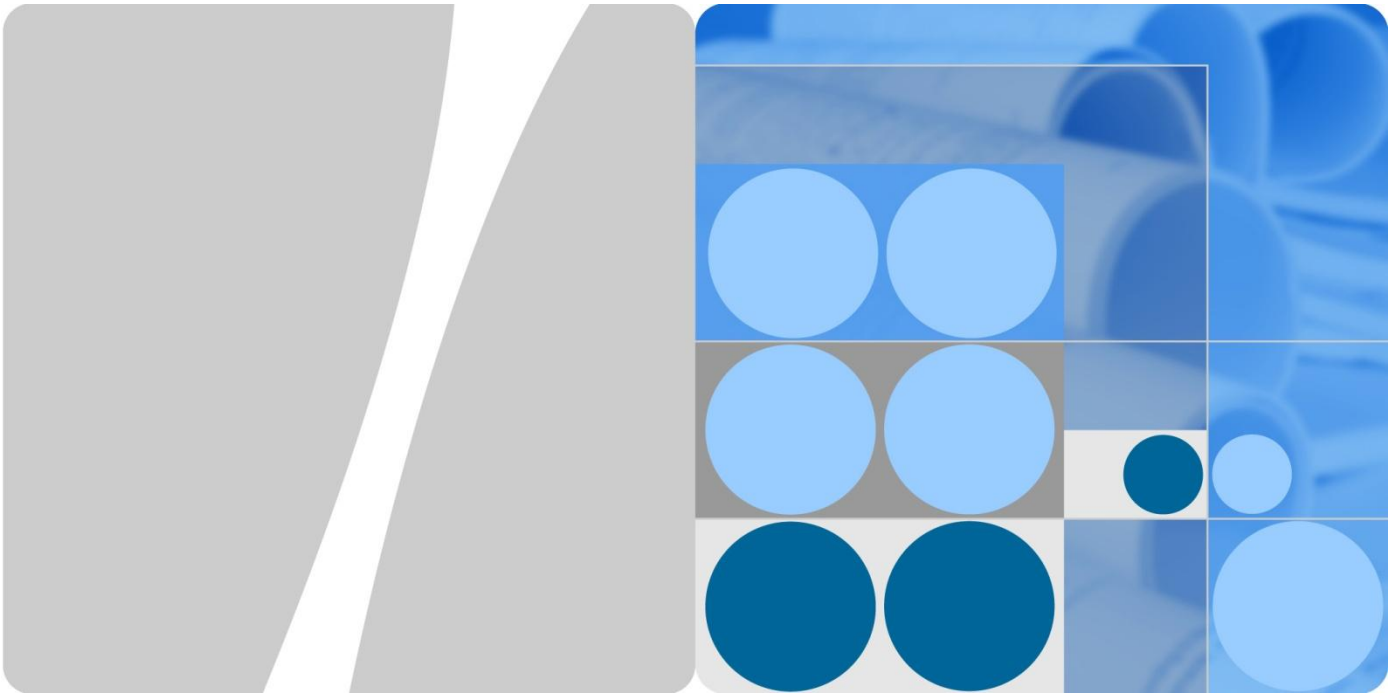


端口安全技术白皮书

文档版本 01

发布日期 2012-8-31

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 端口安全

关于本章

1.1 介绍

端口安全（Port Security）功能将交换机接口学习到的 MAC 地址变为安全 MAC 地址（包括安全动态 MAC 和 Sticky MAC），可以阻止除安全 MAC 和静态 MAC 之外的主机通过本接口和交换机通信，从而增强设备安全性。

1.2 原理描述

端口学习安全 MAC 地址的方式

安全 MAC 地址分为两种：安全动态 MAC 与 Sticky MAC。二者定义及区别如下：

- 安全动态 MAC 地址：使能端口安全而未使能 Sticky MAC 功能时学习到的 MAC 地址。缺省情况下，安全动态 MAC 地址不会被老化，设备重启后安全动态 MAC 地址会丢失，需要重新学习。
- Sticky MAC 地址：使能端口安全后又使能 Sticky MAC 功能后学习到的 MAC 地址。Sticky MAC 地址不会被老化，保存配置后重启设备，Sticky MAC 地址不会丢失，无需重新学习。

未使能接口安全功能时，设备的 MAC 地址表项可通过动态学习或静态配置。当某个端口使能端口安全功能后，该端口上之前学习到的动态 MAC 地址表项会被删除，之后学习到的 MAC 地址将变为安全动态 MAC 地址，此时该端口仅允许匹配安全 MAC 地址或静态 MAC 地址的报文通过。若接着使能 Sticky MAC 功能，安全动态 MAC 地址表项将转化为 Sticky MAC 表项，之后学习到的 MAC 地址也变为 Sticky MAC 地址。直

到安全 MAC 地址数量达到限制，将不再学习 MAC 地址，并对接口或报文采取配置的保护动作。

安全 MAC 地址学习数限制

缺省情况下，每个接口仅可以学习一个安全 MAC 地址，用户可以配置接口学习安全 MAC 地址的最大数量限制。

端口安全保护动作

用户可以配置端口安全的保护动作，当端口学习到的安全 MAC 地址数量达到限制时，可以选择采取以下某一种动作：

- **protect**：当学习到的 MAC 地址数达到接口限制数时，接口丢弃源地址在 MAC 表以外的报文。
- **restrict**：当学习到的 MAC 地址数超过接口限制数时，接口丢弃源地址在 MAC 表以外的报文，并同时发出告警。
- **shutdown**：当学习到的 MAC 地址数超过接口限制数时，接口执行 Shutdown 操作，同时发出告警。

缺省情况下，端口安全保护动作为 **restrict**。

手动指定安全 MAC 地址表项

用户可以通过命令 **port-security mac-address sticky** 手动配置 **sticky-mac** 表项。

说明
本文中的配置命令及配置文件均以 S7700 交换机举例。

安全动态 MAC 的配置

在使用端口安全之前，请确保已完成以下任务：

- 关闭基于接口的 MAC 地址学习限制功能。
- 关闭配置 MUX VLAN 功能。
- 关闭 MAC 认证功能。
- 关闭 802.1x 认证功能。
- 关闭 DHCP Snooping 的 MAC 安全功能。

1. 配置接口 GE1/0/1 的端口安全功能。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security enable
```

2. 配置安全 MAC 学习数量限制为 5，并配置接口的保护动作为 shutdown。

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-num 5
[Switch-GigabitEthernet1/0/1] port-security protect-action shutdown
```

3. 使用 display mac-address security 命令查看安全动态 MAC 地址学习情况。

```
[Switch] display mac-address  security
--------------------------------------------------------------------------------
```

```
MAC Address    VLAN/VSI                    Learned-From       Type
--------------------------------------------------------------------------------
0019-21db-25a3 1/-                         GE1/0/1            security

--------------------------------------------------------------------------------
Total items displayed = 1
```

Sticky MAC 的配置

在使用端口安全之前，请确保已完成以下任务：

- 关闭基于接口的 MAC 地址学习限制功能。
- 关闭配置 MUX VLAN 功能。
- 关闭 MAC 认证功能。
- 关闭 802.1x 认证功能。
- 关闭 DHCP Snooping 的 MAC 安全功能。

1. 配置接口 GE1/0/2 的端口安全功能，并使能 Sticky MAC 功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port-security enable
[Switch-GigabitEthernet1/0/2] port-security mac-address sticky
```

2. 配置安全 MAC 学习数量限制为 5，并配置接口的保护动作为 shutdown。

```
[Switch-GigabitEthernet1/0/2] port-security max-mac-num 5
[Switch-GigabitEthernet1/0/2] port-security protect-action shutdown
```

3. 在接口 GE1/0/2 上手动添加 MAC 地址为 0001-0001-0001、VLAN2 的 Sticky MAC 表项。

```
[Switch-GigabitEthernet1/0/2] port-security mac-address sticky 0001-0001-
0001 vlan  2
```

4. 使用 display mac-address sticky 命令查看 Sticky MAC 地址学习及配置情况。

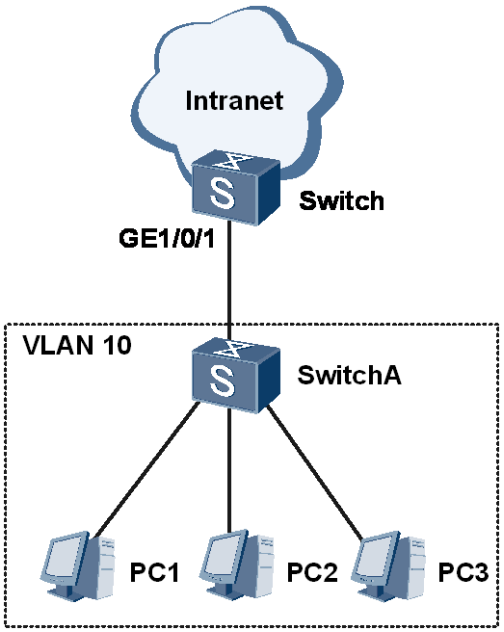
```
[Switch] display mac-address  sticky
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI                    Learned-From       Type
--------------------------------------------------------------------------------
0025-9eff-ffff 1/-                         GE1/0/2            sticky
0001-0001-0001 2/-                         GE1/0/2            sticky

--------------------------------------------------------------------------------
Total items displayed = 2
```

1.3 应用

1.3.1 端口安全典型组网应用

如图 1-1 所示，公司为了提高信息安全，将 Switch 连接用户侧的接口使能了端口安全功能，并且设置了接口学习 MAC 地址数的上限为信任的设备总数，这样其他外来人员使用自己带来的 PC 无法访问公司的网络。

图1-1 配置端口安全示例组网图



Switch 的配置文件。

```
#
 sysname Switch
#
 vlan batch 10
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 port-security enable
 port-security protect-action protect
 port-security max-mac-num 4
 port-security mac-address sticky
#
return
```