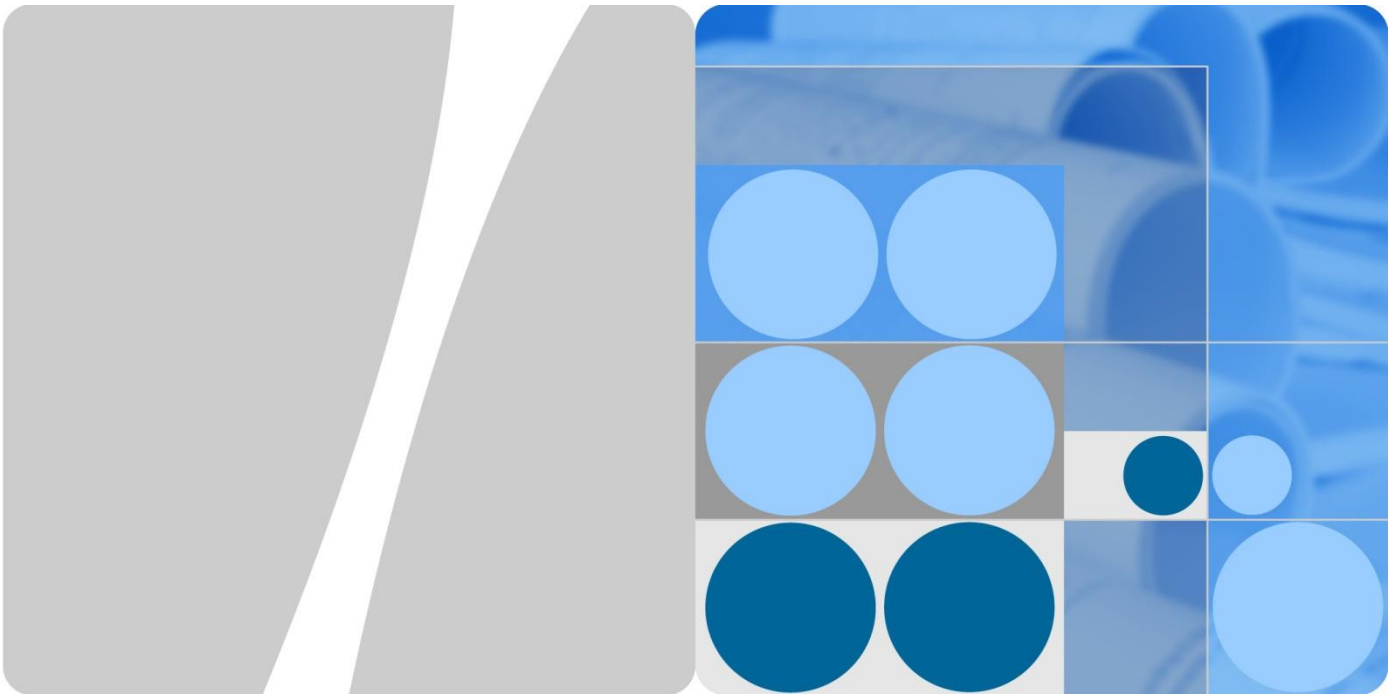


Port Security Technology White Paper

Issue 01

Date 2012-08-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Port Security

About This Chapter

1.1 Introduction to Port Security

The port security function changes MAC addresses learned on an interface into secure MAC addresses (including secure dynamic MAC addresses and sticky MAC addresses). Only hosts using secure MAC addresses or static MAC addresses can communicate with the switch through the interface. This function enhances security of the switch.

1.2 Principles

Secure MAC Address Learning

Secure MAC addresses include secure dynamic MAC addresses and sticky MAC addresses. Differences between secure dynamic MAC addresses and sticky MAC addresses are as follows:

- Secure dynamic MAC addresses are learned on an interface where port security is enabled but the sticky MAC function is disabled. By default, secure dynamic MAC addresses will never be aged out. After the switch restarts, secure dynamic MAC addresses are lost and need to be learned again.
- Sticky MAC addresses are learned on an interface where both port security and sticky MAC function are enabled. Sticky MAC addresses will not be aged out. After you save the configuration and restart the switch, sticky MAC addresses still exist.

Before port security is enabled on an interface, MAC address entries can be configured statically or learned dynamically on the interface. After port security is enabled on an interface, dynamic MAC address entries that have been learned on the interface are deleted

and MAC address entries learned subsequently turn into secure dynamic MAC address entries. Only packets with source MAC addresses matching the secure dynamic MAC address entries or static MAC address entries can pass through the interface. After the sticky MAC function is enabled on the interface, existing secure dynamic MAC address entries and MAC address entries learned subsequently on the interface turn into sticky MAC address entries. When the number of secure MAC addresses reaches the limit, the switch stops learning MAC addresses on the interface and takes a protection action on the interface or packets received.

Maximum Number of Secure Dynamic MAC Addresses

By default, only one secure MAC address can be learned on an interface. You can set the maximum number of secure MAC addresses that can be learned on an interface.

Port Security Protection Action

You can configure a protection action for port security for the switch to perform when the number of secure MAC addresses learned on an interface reaches the maximum number. The switch supports the following protection actions:

- **protect**: discards packets with new source MAC addresses.
- **restrict:** discards packets with new source MAC addresses and sends a trap.
- **shutdown**: shuts down the interface and sends a trap.

The default action is **restrict**.

Manually Configuring a Sticky MAC Address Entry

You can use the **port-security mac-address sticky** command to configure a sticky MAC address entry.

NOTE

This document uses the commands and configuration file of the S7700 switch as an example.

Configuring Secure Dynamic MAC Address Learning

Before configuring port security on an interface, complete the following tasks:

- Disable MAC address limiting on the interface.
- Disable the MUX VLAN function on the interface.
- Disable MAC address authentication on the interface.
- Disable 802.1x authentication on the interface.
- Disable MAC security for DHCP snooping.

Step 1 Enable port security on GE1/0/1.

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

Step 2 Set the maximum number secure MAC addresses on the interface to 5 and set the protection action to shutdown.

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

Step 3 Run the **display mac-address security** command to check the secure dynamic MAC address entries learned on the interface.

```
[Switch] display mac-address  security
-------------------------------------------------------------------------------
MAC Address   VLAN/VSI                      Learned-From       Type
-------------------------------------------------------------------------------
0019-21db-25a3 1/-                          GE1/0/1            security

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

----End

Configuring the Sticky MAC Function

Before configuring the sticky MAC function on an interface, complete the following tasks:

- Disable MAC address limiting on the interface.
- Disable the MUX VLAN function on the interface.
- Disable MAC address authentication on the interface.
- Disable 802.1x authentication on the interface.
- Disable MAC security for DHCP snooping.

Step 1 Enable port security and sticky MAC on GE1/0/2.

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

Step 2 Set the maximum number secure MAC addresses on the interface to 5 and set the protection action to shutdown.

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

Step 3 Add a sticky MAC address entry on GE1/0/2, in which the MAC address is 0001-0001-0001 and VLAN ID is 2.

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

Step 4 Run the **display mac-address sticky** command to check the learned and manually configured sticky MAC address entries.

```
[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
```

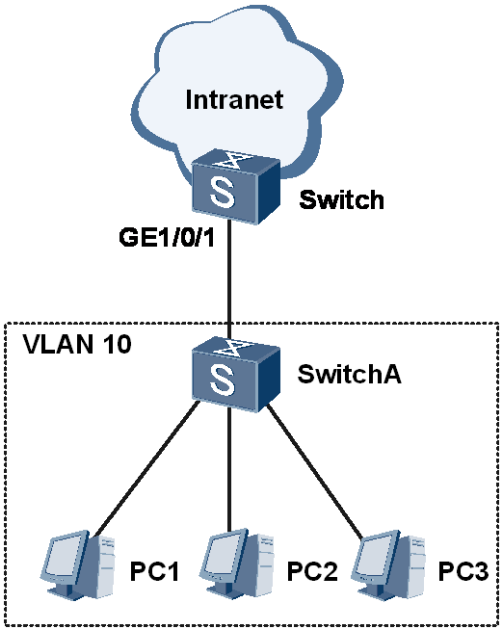
----End

1.3 Applications

1.3.1 Typical Application of Port Security

As shown in Figure 1-1, a company wants to prevent PCs of non-employees from accessing the intranet to protect information security. To achieve this goal, the company needs to enable the sticky MAC function on the user-side interface GE1/0/1 of Switch and set the maximum number of secure MAC addresses learned on the interface to be the same as the number of trusted devices.

Figure 1-1 Typical application of port security



Configuration file of Switch

```
#
 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
```