Port Additional Characteristic Configuration

Table of Contents

Chapter 1 Port Security

1.1 Introduction

You can control the access function of the secure port, enabling the port to run in a certain range according to your configuration. If you enable the security function of a port through configuring the number of secure MAC addresses for the port. If the number of secure MAC addresses exceeds the upper limitation and MAC addresses are insecure, secure port violation occurs. You should take actions according to different violation modes.

The secure port has the following functions:

- Configuring the number of secure MAC addresses
- Configuring static secure MAC addresses
  If the secure port has no static secure MAC address or the number of static secure MAC addresses is smaller than that of secure MAC addresses, the port will learn dynamic MAC addresses.
- Dropping violated packets when secure port violation occurs

The section describes how to configure the secure port for the switch.

1.2 Configuring Secure Port Task List

- Configure MAC addresses and the binding of IP address.

1.3 Configuring Secure Port Task

1.3.1 Configuring MAC Address and Binding of IP Address

The switch can bind both the IP address and the MAC address to the port, or just bind one of them.

Note:

After the IP address is bound to the MAC address on the port, IP messages that are incompatible with the bound MAC addresses are to be filtrated.

Enter the port configuration mode and run the following command to display the configuration information about secure port.

Run…	To…
switchport port-security bind {**ip** *A.B.C.D* **| mac** *H.H.H*}	Bind the IP address to the MAC address on the port.

Chapter 2 Port Congestion

In normal case, the Ethernet interface will broadcast unknown message to the VLAN where the Ethernet interface is located. In some cases, message of the type is forbidden to forward.

Command	Description
switchport block {**unicast**|**multicast**| **broadcast**}	The interface does not forward uni-cast, multicast or broadcast message.
no switchport block {**unicast** | **multicast** | **broadcast**}	The interface forwards all message.

Chapter 3 Port Protection

In normal cases, packets between different ports on a switch can be freely forwarded. In some cases, packets between different ports are not allowed to forward. The port isolation function can forbid the packet flow between ports. The ports with the isolation function cannot communicate with each other. Packets can be normally forwarded between ports without isolation function or between isolated ports and non-isolated ports.

Command	Description
switchport protected	Sets port isolation.
no switchport protected	Cancels port isolation.

Chapter 4 Port Storm Control

The port of switch may bear continuous and abnormal attack from Uni-cast (fail to look up the MAC address), multicast or broadcast message. In this case, the port of the switch or the whole switch will break down. A mechanism must be provided to constrain the phenomena.

Command	Description
storm-control {**broadcast** | **multicast** | **unicast**} **threshold count**	Controls the storm of broadcast, multicast or uni-cast message.
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**	Does not control the storm.

Chapter 5 Port Rate Limitation

You can control the rate of outward/inward traffic through configuration.

Run the following commands in privilege mode to control the traffic rate of the port:

Run…	To…
configure	Enter the global configuration mode.
interface g0/1	Log in to the to-be-configured port.
[**no**] **switchport rate-limit** *band* { ingress|egress}	Configure the traffic rate control for a port. **band** is the traffic rate to be controlled. **ingress** means having effect on the incoming port. **egress** means having effect on the outcoming port.
exit	Enter the global configuration mode again.
exit	Enter the management configuration mode again.

Chapter 6 Port Loop Detection

You can detect whether loop occurs on the port through configuration.

Enter the port configuration in global configuration mode:

Command	Description
[no] keepalive	(Disables) enables port loop detection.
keepalive *period*	Sets the period for port loop detection. Its effective range is from 0 to 32767.