Port Additional Characteristics Configuration

Table of Contents

Chapter 1   Port Security

1.1   Configuring the Maximum Number of Dynamic MAC Addresses for the Secure Port

The number of secure MAC addresses on the secure port is that of the MAC addresses that can be learned as many as possible. If the number of source MAC addresses exceeds the specified number, the violation of the secure port may occur. The default value is **1**.

Run the following commands in EXEC mode to configure the MAC address of the secure port:

Command	Purpose
configure	Enters the global configuration mode.
interface f0/1	Enters the to-be-configured port.
[**no**] **switchport port-security dynamic maximum** *value*	Specifies/cancels the maximum number of dynamic MAC addresses of maximum secure ports. The parameter **value** represents the maximum number of the configured MAC addresses.
exit	Exits the global configuration mode.
exit	Exits the management configuration mode.
write	Saves the configuration.

1.2   Configuring Static MAC Addresses of the Secure Port

After the static MAC address of the secure port is configured, no security violation will occur on the packet if the incoming MAC address is a static one.

Run the following commands in EXEC mode to configure the static MAC address:

Command	Description
configure	Enters the global configuration mode.
interface f0/1	Enters the to-be-configured port.
[**no**] **switchport port-security mac-address** *mac-addr*	Adds/deletes the secure static MAC address on the secure port. ● *mac-addr* stands for the configured MAC address.
exit	Exits the global configuration mode.
exit	Exits the EXEC mode.

write	Saves the configuration.

Chapter 2 Port Protection

Normally, the packets can be freely forwarded between different ports of the switch. In some cases, the data flow is forbidden between the ports through the port segregation function. The packet communication does not exist between the segregated ports, while it exists between the unsegregated ports or between segregated port and unsegregated port.

Command	Purpose
switchport protected	Sets the port segregation.
no switchport protected	Cancels the port segregation.

- 4 -

Chapter 3   Port Storm Control

The ports of the switch may receives the attack by the continuous abnormal unicast (MAC address lookup failing), multicast or broadcast message. In this case, the attacked ports or the whole switch may break down. The storm control mechanism of the port is therefore generated.

If n<=28, the expression is n*64Kbps.

If n>28, the expression is (n-27)Mbps.

Command	Purpose
storm-control {**broadcast** | **multicast** | **unicast**} **threshold count**	Performs the storm control to the broadcast/multicast/unicast message.
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**	Cancels the storm control.

Chapter 4   Port Speed Limitation

You can limit the incoming/outgoing flow rate of the port.

Run the following commands in privileged mode to limit the flow rate of the port.

Command	Purpose
configure	Enters the global configuration mode.
interface f1/0	Enters the to-be-configured port.
[no] switchport rate-limit *band* { ingress|egress}	Configures the flow rate limits for the port. The parameter **band** represents the to-be-limited flow rate. The parameter **ingress** means the function works at the incoming port. The parameter **egress** means the function works at the outgoing port.
exit	Exits the global configuration mode.
exit	Exits the management configuration mode.