Port Additional Characteristic Configuration

Contents

Chapter 1   Interface Configuration

1.1   Configuring Ethernet Interface

It provides the information about Ethernet interface configuration procedures in this chapter.10Mbps Ethernet and 100Mbps Fast Ethernet interface are supported on our switch. Configuration steps are listed as follow. The first step is mandatory and the others are optional.

1.1.1   Configuring Port Loop Examination

Port sends keepalive packets after configure keepalive functions on port, to realize loop examination.

Command	Purpose
keepalive *period*	Enable keepalive function on port *Period* specifies the interval of loopback packets sent by port。
no keepalive	Disable keepalive function.

1.1.2   Configuring Port Rate Limit

Use the following configuration commands to limit ports rate.

Enter the privilege mode,

Command	Purpose
Configure	Enter global configuration mode
interface f0/0	Enter the port to be configured.
[**no**] **switchport rate-limit** *band* **ingress** }	Configure ports rate limit *band*, specifies the rate that you want to limit. ingress indicates it is valid to ingress. egress, indicates it is valid to an egress
exit	Return to global configuration mode
exit	Return to administration configuration mode

1.1.3   Configuring Interface Flow Control

In full duplex mode, flow control is implemented with PAUSE frame defined in 802.3X; and in half duplex mode with back pressure

Command	Description
flow-control on/off	Enable/Disable interface flow control.
no flow-control	Restore to default settings without interface flow control

1.1.4   Configuring Port Storm-control

A persistent and abnormal packets storm arisen from a broadcast, a multicast or a unicast(MAC address searching is abort) might occur on one of the physical interfaces, which may bring on the failure of physical ports or even the whole switch. Therefore, it is important to provide a mechanism to suppress the packets storm.

Command	Purpose
**storm-control {broadcast	multicast } threshold count**	Implement packets storm-control on broadcast/multicast/
**no storm-control {broadcast	multicast } threshold**	Stop storm-control

Chapter 2   Port Security Configuration

2.1   Overview

Port security can control accessing to ports so that it can be enabled to be used within a certain scope configured by user. By configuring security MAC address number on each port, the security MAC address function is enabled. If the entered MAC address is not security address and the number of them is over the maximum threshold at the same time, which is called port-security violation. Afterwards the remedy will be triggered according to different violation modes.

Port security provides the following features: configurable security MAC address number and configurable static security MAC address. If static security MAC address is not defined or static security MAC address number is less than defined address number on this security port, dynamic security Mac address learning will be started up. If port-security violation occurs, violated packets will be thrown away until violation is cleared.

This chapter provides the information about security interface configuration on our switch.

2.2   Configuring Security Interface Tasks List

- Enabling/Disabling port security

- Configuring port-security violation mode

- Configuring security MAC address number

- Configuring static security MAC address

- Configuring address aging time of port security

- Displaying security interface configuration information

- Displaying MAC address information

- Configuring the binding of MAC address and IP address

2.3   Configuring Security Interface Tasks

2.3.1   Enabling/Disabling port security

Default setting: disable port security

Port security is also disabling in aggregation ports and member of trunk.

Enter administration mode, configure port security as follow:

Command	Purpose

configure	Enter global configuration mode
interface f0/1	Enter the port to be configured.
[**no**] **switchport** *port-security*	Enable/Disable port security.
exit	Return to global configuration mode
exit	Return to administration configuration mode
write	Save configuration

2.3.2　Configuring port-security violation mode

If violation occurs after disable port security, the remedy will be triggered according to different violation modes.

Default violation mode: protect.

Enter administration mode, configure port security violation mode as follow:

Command	Purpose
configure	Enter global configuration mode
interface f0/1	Enter the port to be configured.
[**no**] **switchport port-security violation** [*protect*|*restrict*]	Configure port-security violation mode ● *protect mode:* no report ● *restrict mode:* report error message
exit	Return to global configuration mode
exit	Return to administration configuration mode
write	Save configuration

2.3.3　Configuring static security MAC address

Data packets will not result in violation when the entry MAC address is configured static security MAC address.

Enter administration mode, configure static security MAC address as follow:

Command	Purpose
configure	Enter global configuration mode
interface f0/1	Enter the port to be configured.
[**no**] **switchport port-security mac-address** *mac-addr*	`Add/delete static security MAC address` ● *mac-addr:* configured MAC address
exit	Return to global configuration mode
exit	Return to administration configuration mode
write	Save configuration

2.3.4   Displaying security interface configuration information

Show the configuration information of one or all security interface by "show" command, including the security interface number, MAX number of MAC, the number of MAC address learnt by active port, the number of port-violation.

Enter administration mode, use the following commands to show the port security configuration information:

Command	Purpose
show port-security [interface *interface-id***]**	Display security interface configuration information ●*interface-id:* ID number of the interface

2.3.5   Displaying MAC address information

Show the configuration information of one or all security interface by "show" command, including static security MAC address and dynamic learnt MAC address.

Enter administration mode, use the following commands to show the MAC address information:

Command	Purpose
show mac address-table [interface *interface-id*]	Display security interface MAC address information ● *interface-id:* ID number of the interface

2.3.6   Configuring the binding of MAC Address and IP Address

For this kind of switch, you can bind IP address and MAC address on a port at the same time, or bind IP and MAC separately.

Note:

Once MAC address and IP address binding is configured, all the IP packet which is not matched with bound address will be filtered.

Enter port configuration mode and use the following command to display port security configuration information.

Command	Description
switchport port-security bind {ip *A.B.C.D* **| mac** *H.H.H*}	Configure binding of MAC and IP address on the port.

Chapter 3   Interface Configuration Example

3.1   Configuring Interface Attributes

3.1.1   Interface Description Example

The following example indicates how to add an interface description entry which will appear in configuration file and interface display command.

interface vlan 1
ip address 192.168.1.23 255.255.255.0

3.1.2   Examples

The following example shows how to stop the Ethernet interface on port 1.
interface fastEthernet 0/1
flow-control on

The following example shows how to restart an interface.
interface fastEthernet 0/1
flow-control off