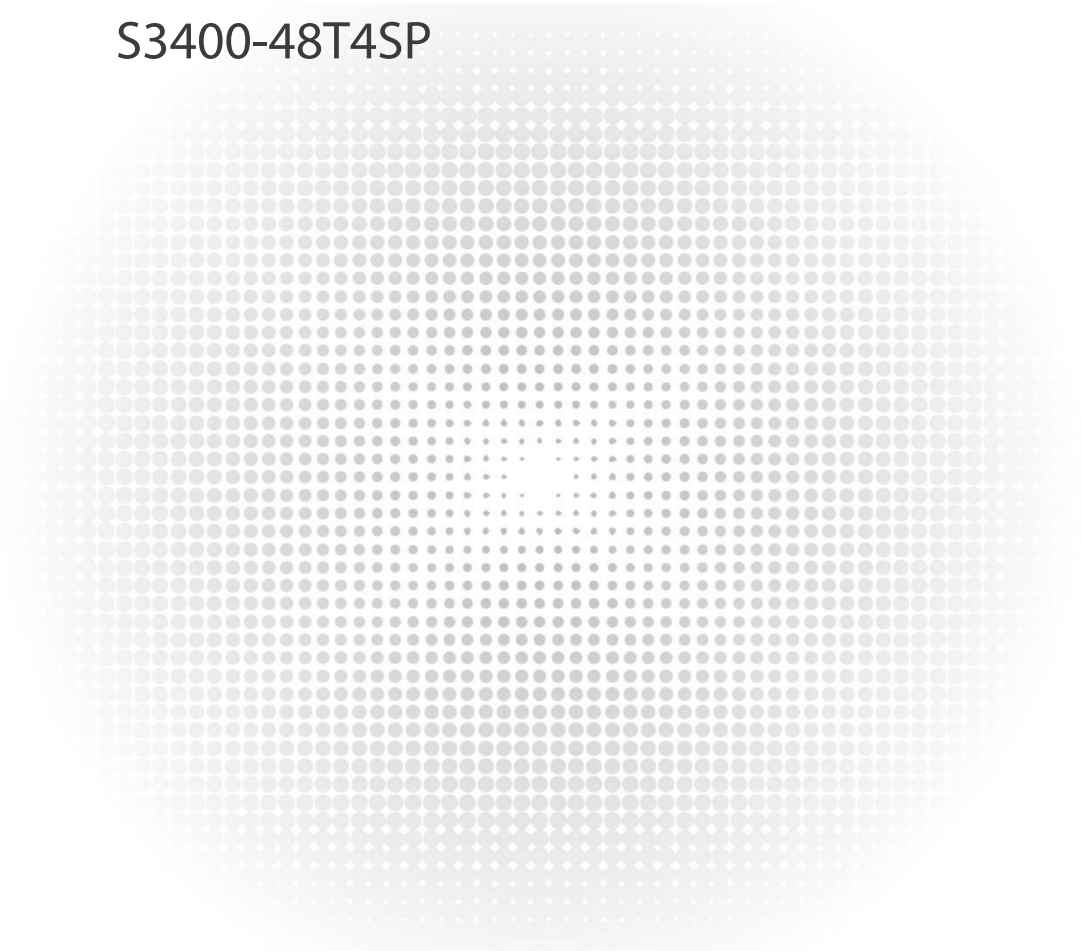
PoE+ Series Switches Port Additional Characteristics Configuration Guide

Models: S3150-8T2FP
S3260-8T2FP
S3260-16T4FP
S3400-24T4FP
S3400-48T4SP



CONFIGURATION GUIDE

Contents

Chapter 1 Port Additional Characteristics Configuration

1.1 Port Isolation

Generally, the packets between different ports of a switch can be freely forwarded. In some cases, the data flows between ports need be forbidden and port isolation is then required. Data communication cannot go on between isolated ports, but can do between normal ports or between normal port and isolated port. Data communication cannot go on between the isolated ports within one group, but can do between the isolated port and any arbitrary port outside the group. It is noted that port isolation plays a role in the layer-2 packets. This switch series does not support group-based isolation.

Isolation not based on the group:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport protected**	Enable or disable Port Isolation
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Isolation based on the group:

Command	Purpose
config	Enters the global configuration mode.
[no] **port-protected** *group-id*	Creates and enters the isolation group mode, run this command. Sets ID of the isolation group
[no] **description** *word*	Describes the group. Word Describes the character string of the group.
exit	Goes back to the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport protected** *group-id*	Add/remove the isolation group *group-id*The isolation group ID
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.2 Storm Control

The port of a switch may bear continuous and abnormal impact from unicast (MAC address fails to be found), multicast or broadcast packets, and therefore gets paralyzed even to the extent that the whole switch breaks down. That's why a mechanism must be provided to limit this phenomena. The storm control enables the OLT to set on the ingress the rates of different kinds of packets.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **storm-control** {**broadcast** | **multicast** | **unicast**} **threshold** *count*	Sets flow control for a port. unicast means that storm control is conducted to the unicast packets. multicast means that storm control is conducted to the multicast packets. **broadcast** means that storm control is conducted to the broadcast packets. Count means the threshold of the being configuration
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3 Rate Control

Rate limit is used to limit the rate of a flow that runs through a port. Enter the privileged mode and run the following commands to limit the rate of a port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport rate-limit** {*band* | ***bandwidth*** *percent*} { **ingress**|**egress**}	Configures the rate limit for a port. Band means to limit the flow rate. *percent*means to limit the flow percentage. ingress means to exert an influence on the ingress. egress means to exert an influence on the egress.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.4 Loopback Detection

Loopback detection is used to check whether loopback exists on an interface. You can configure the interval for a port to transmit the loop check packets. Enter the privileged mode to run the following commands to set the interval for the port to transmit loopback detection packets.

Command	Purpose
config	Enters the global configuration mode.
Interface g0/1	Enters the to-be-configured port.
[no] **keepalive** [*second*]	To configure the interval for a interface to transmit the loop check packets, run keepalive second. To return to the default setting, use the no form of this command. second means the interval of transmitting the packets.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.5 MAC Address Learning

MAC address learning is used to enable or disable MAC addresss learning on the interface. The configuration method is shown as follows:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport disable-learning**	Sets MAC address learning on a port. Enables/disables interface MAC address learning.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.6 Port Security

Port security supports security control on an interface. Port security has four modes: dynamic security mode, static reception mode, static rejection mode and sticky security mode. In dynamic security mode, you can set the threshold of MAC addresses that can be learned by a port. If the learned MAC addresses on a port have reached the threshold in number, the switch will not learn the MAC addresses any more and at the same time drop all DLF packets. In static security mode, you can set the static security MAC address on a port and then you should consider three cases: if it is in static reception mode, only the packets whose destination MACs are security MACs can be allowed to enter this port and other packets will be dropped; if it is in static rejection mode, the packets whose destination MACs are security MACs will be all dropped and other packets will be allowed to pass through this port; if it is in sticky security mode, the mac address of the unknown source unicast packet will be learned to

the sticky mac address. The sticky mac address can be configured manually or dynamically generated. The command "show running-config" can be used to check the sticky mac address. There are two aging modes for the sticky mac address: absolute aging mode and inactivity aging mode. Inactivity, similar to the dynamic aging, is an aging after there is no data traffic. The sticky security mode can set the port allowable learned maximum sticky MAC address number. If the learned MAC addresses on a port have reached the threshold in number, the switch will not learn the MAC addresses any more and at the same time drop all DLF packets.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport port-security mode** {**dynamic | static** *accept|reject* **| sticky**}	Setting the Interface Security Mode **Dynamic** means the dynamic security mode. Static accept means the static reception mode. Static reject means the static rejection mode. **Sticky** means the sticky security mode.
[no] **switchport port-security dynamic maximum** *num*	Sets the maximum number of MAC learning addresses
[**no**] **switchport port-security static mac-address** *H.H.H*	Configures a static security MAC address.
[**no**] **switchport port-security sticky** {**maximum** *sticky_number* | **mac-address** *H.H.H* | **aging-time** *aging_time* | **absolute-aging** | **inactivity-aging**}	Configures the sticky characteristic of MAC address, run this command. **maximum** *sticky_number* means the maximum number of sticky mac address **mac-address** *H.H.H* means configure the sticky mac address manually **aging-time** *aging_time* means configuring the aging time of the sticky mac address **absolute-aging** means configuring the absolute aging mode(default) **inactivity-aging** means configuring the aging mode of inactivity
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.7 Port Binding

This type of switches can bind the IP address and the MAC address to a port at the same time, and of course you can bind either one to the port. Port binding is effective to the IP or ARP packets.

Use the following command in interface configuration mode:

Command	Purpose

config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] **switchport port-security bind|block** {**ip|arp| both-arp-ip** *A.B.C.D* **| mac** *H.H.H* **| ipv6** *ipv6_addr*}	Configures Port Binding bind means that only the packets that comply with the binding requirements can pass while other packets will be dropped; block means that only the packets that comply with the binding requirements will be rejected and other packets will pass. Ip means the relative action, rejection or reception, is effective to the Ip packets that comply with the binding requirements. Arp means the relative action, rejection or reception, is effective to the ARP packets that comply with the binding requirements. both-arp-ip means effective to the IP and ARP packets that comply with the binding requirements. Ipv6means effective to the Ipv6 packets that comply with the binding requirements.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.8 SVL/IVL

The switch can configure SVL or IVL mode. It is IVL mode by default. The settings is shown as follows:

Command	Purpose
config	Enters the global configuration mode.
[no]**vlan shared-learning**	Sets SVL/IVL
exit	Goes back to the EXEC mode.

1.9 Configuring Link scan

1.9.1 Overview

The command is used to scan the time interval on the port. You can fast scan the up/down state on the port.

1.9.2 Link Scan Configuration Task

- Configure the time interval on the port.

1. Set the time interval of port scan

To set the scan interval of an interface, run the following command in the global configuration mode:

Command	Purpose
[no] Link scan [normal | fast] *interval*	Normal means standard link scan mode. Fast means fast link scan mode. Fast mode is mainly used for service protocol requirement, such as rstp. Configure the time interval on the port.

1.9.3 Configuration Example

The following example shows how to set the scan interval to 20ms.

link scan normal 20

1.10 Configuring the Enhanced Link State Detection Command

1.10.1 Overview

Configuring the enhanced link state detection of the port and fastly checking the link state of the port.

1.10.2 Configuration Tasks

- To enable/disable the enhanced link state detection command, run the following command.

1. To enable/disable the enhanced link state detection command, run the following command.

In port configuration mode, run the following commands respectively to enable or disable the enhanced link state detection:

Command	Purpose
[no] switchport enhanced-link	To enable/disable the enhanced link state detection command, run the following command.

1.10.3 Configuration Example

The following example shows how to enable the enhanced link state detection on interface g0/1:
Switch_config#interface g0/1
Switch_config_g0/1#switchport enhanced-link

1.11 Configuring System MTU

1.11.1 Overview

Configuring system mtu

1.11.2 Configuration Tasks

- Configuring system mtu

1. Set system mtu.

Run the following command in the global configuration mode:

Command	Purpose
[no] system mtu *mtu*	To set the value of system mtu, run this command.

1.11.3 Configuration Example

The following example shows how to set system mtu to 2000 bytes.

Switch_config#system mtu 2000