

Port's Additional Features Configuration

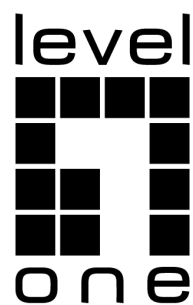


Table of Contents

Chapter 1	Port's Additional Features Configuration.....	1
1.1	Storm Suppression.....	1
1.2	Port Isolation	1
1.3	Storm Control	1
1.4	Port's Rate Limitation	2
1.5	Port Loop Detection.....	2
1.6	Port MAC-address learning	3
1.7	Port's Security	3
1.8	Interface's binding	4
1.9	SVL/IVL	4
1.10	VLAN MAC Address Learning	4
1.11	Number of VLAN MAC addresses learned	5
1.12	Configuring Link Scan	5
1.12.1	Overview	5
1.12.2	Link scan configuration tasks	5
1.12.3	Set the port scan interval	5
1.12.4	Configuration Example	5
1.13	Configuring system mtu.....	6
1.13.1	Overview	6
1.13.2	Configuration Task.....	6
1.13.3	Configuring system mtu	6
1.13.4	Configuration Example.....	6

Chapter 1 Port's Additional Features Configuration

1.1 Storm Suppression

Actually, the Ethernet interface may receive unknown packets (DLF packets). The switch broadcasts this type of packets to all ports in the VLAN by default, which will increase the load on the network and affect the performance of the network. In order to avoid this situation, set the DLF message to be discarded at the egress of the message. This is the storm suppression.

Command	Purpose
config	Entering global configuration mode
interface g0/0/1	Entering the interface which to be configured
[no] switchport block {unicast multicast broadcast}	Configure the storm speed limit function of the port. Unicast means that it works on unknown unicasts. multicast means that it works on multicast t; Broadcast means to play a role in broadcasting.
exit	Back to global configuration mode
exit	Back to management configuration mode

1.2 Port Isolation

Under normal condition, data packet could be forwarded among different ports of switches. Under some circumstances, flows among ports need to be forbidden, and port isolation function is the one to provide this kind of control. For isolation which is not based on group, data communication could not work between isolated ports, but data packets among non-isolated ports and isolated and non-isolated ports could be forwarded normally.

Command	Purpose
config	Entering global configuration mode
interface g0/0/1	Entering the interface which to be configured
[no] switchport protected	Enable/cancel port isolation function
exit	Back to global configuration mode
exit	Back to management configuration mode

1.3 Storm Control

Switch's ports could be attacked by constant abnormal unicast (MAC address locating failure), multicast or broadcast messages. It might cause switch's ports and even the whole switch's failure. Therefore, a mechanism has been provided to restrain this phenomenon. Storm control function could set different rates at the ingress for different kinds of messages which are allowed to enter switch.

Command	Purpose
config	Entering global configuration mode

interface g0/0/1	Entering the interface which to be configured
[no] storm-control { mode broadcast multicast unicast } { kpps pps threshold count action action_select auto_resume time }	Configuring port's storm control function. Mode indicates the storm control rate statistics mode unicast means it works for unknown unicast. multicast means it works for multicast. broadcast means it works for broadcast. <i>count</i> indicates the to-be-configured threshold. action indicates the action after the threshold is reached. <i>action_select</i> indicates the to-be-configured operation. auto_resume indicates automatic recovery. <i>time</i> indicates auto recovery time.
exit	Back to global configuration mode
exit	Back to management configuration mode

1.4 Port's Rate Limitation

Port's rate limitation is used for limiting the rate of flow which comes in and goes out of ports. Use the following commands to limit port's flow rate after entering management mode:

Command	Purpose
config	Entering global configuration mode
interface g0/0/1	Entering the interface which to be configured
[no] switchport rate-limit { <i>band</i> Bandwidth percent } { ingress egress } burst-size <i>high</i> <i>middle</i> <i>low</i> }	Configuring the flow rate limitation for port. Band is the limited flow rate. <i>Percent</i> is the limited flow percentage. Ingress means it works for ingress; Egress means it works for egress. burst-size means the matching packet buffer. <i>high, middle, low</i> means the size of the message buffer
exit	Back to global configuration mode
exit	Back to management configuration mode

1.5 Port Loop Detection

Port loop detection function is used for detecting whether port has loop. Time interval of loop detection messages sent by port could be configured. Use the following command to set time interval of loop detection messages sent by port after entering management mode.

Command	Purpose
config	Entering global configuration mode
Interface g0/0/1	Entering the interface which to be configured
[no] keepalive [<i>second</i>]	Configuring time interval of loop detection messages sent by port.

	<i>Second</i> is the time interval of sending messages.
exit	Back to global configuration mode
exit	Back to management configuration mode

1.6 Port MAC-address learning

Port MAC address learning is used to enable/disable port MAC address learning. The configuration method is as follows:

Command	Purpose
config	Entering global configuration mode
interface g0/0/1	Entering the interface which to be configured
[no] switchport disable-learning	Configure port MAC address learning. Enable/disable port MAC address learning function.
exit	Back to global configuration mode
exit	Back to management configuration mode

1.7 Port's Security

Port's security does controlling by accessing port according to MAC address. Port's security has three kinds of modes: dynamic security mode, static accepting mode, and static rejecting mode. Under dynamic security mode, maximum MAC address quantity which is allowed to be learnt by ports can be configured. When the maximum mac quantity has been learnt from some port by switch, mac address would not be learnt; at the meantime, switch drops all the DLF messages. Under static security mode, static security MAC address can be configured at port. Under static accepting mode, only messages which source MAC is safe MAC address are allowed to get in, and others would be dropped. Under static rejecting mode, messages which source MAC is safe MAC address would be dropped, and other messages would be allowed to get in.

Command	Purpose
config	Entering global configuration mode
interface g0/0/1	Entering the interface which to be configured
[no] switchport port-security mode {dynamic static {accept reject} }	Configuring port's security mode. Dynamic means dynamic security mode. static accept means static accepting mode static reject means static rejecting mode
[no] switchport port-security dynamic maximum num	Configuring maximum learnable MAC address quantity
[no] switchport port-security static mac-address AA:BB:CC:DD:EE:FF [vlan vlanid]	Configuring static security address
exit	Back to global configuration mode
exit	Back to management configuration mode

1.8 Interface's binding

This switch could be bind with IP address and MAC address on interface at the same time, or be bind with only IP address or MAC address. It works for IP and ARP messages.

Use the following commands to do configuration after entering management mode:

Command	Purpose
config	Entering global configuration mode
interface g0/0/1	Entering the interface which to be configured
[no] switchport port-security bind block {ip arp vlan both-arp-ip A.B.C.D mac AA:BB:CC:DD:EE:FF }	Configuring interface's binding function. Bind only allows messages which conform to binding requirements to pass, and other messages would not be allowed to pass. Block only reject messages which conform to binding requirements, and others would be allowed to pass. Ip means it would only work for IP messages which conform to binding requirements; Arp means it would only work for arp messages which conform to binding requirements; Vlan means that it works for VLAN messages which conform to binding requirements; both-arp-ip means it would work for ip and arp messages conforming to binding requirements.
exit	Back to global configuration mode
exit	Back to management configuration mode

1.9 SVL/IVL

This switch can be configured with Shared (SVL)/independent (IVL) vlan learning mode. By default, the ports are all in IVL mode.

Command	Purpose
config	Entering global configuration mode
[no] vlan shared-learning	Configuring SVL/IVL
exit	Back to management configuration mode

1.10 VLAN MAC Address Learning

The vlanmac address learning command is used to enable/disable the vlan MAC address learning function. The configuration method is as follows:

Command	Purpose
config	Entering global configuration mode
[no] vlan disable-learning add remove word word> <	Prohibit/allow vlan mac address learning. add remove word means to add/delete the vlan that is forbidden to learn the address.

	Word means to prohibit learning address vlan.
exit	Back to management configuration mode

1.11 Number of VLAN MAC addresses learned

By configuring the number of vlan mac addresses to learn, you can control the maximum number of mac addresses that vlan can learn.

The configuration is as follows:

Command	Purpose
config	Entering global configuration mode
[no] vlan dynamic vlan word maximum num	Cancel/Configure the maximum number of learnable vlan mac addresses Word means the vlan of the learning address that needs to be configured. num means the maximum number of mac addresses that can be learned.
exit	Back to management configuration mode

1.12 Configuring Link Scan

1. Overview

Configure the port scan interval to quickly scan the up/down status of the port.

2. Link scan configuration tasks

Configure the port scan interval.

3. Set the port scan interval

When setting up port's scanning time interval, use the following command under global configuration mode:

Command	Purpose
[no] Link scan [normal fast] interval	Normal means standard link scanning mode. Fast means quick link scanning mode. Fast mode mainly applies to service protocol, like rstp. Interval means configuring port's scanning time interval.

4. Configuration Example

The following example shows how to configure the standard scan interval to 20ms:

link scan normal 20

1.13 Configuring system mtu

1. Overview

Configure system mtu

2. Configuration Task

Configure system mtu

3. Configuring system mtu

Use the following command under global configuration mode:

Command	Purpose
[no] system mtu <i>mtu</i>	Configuring system mtu value.

4. Configuration Example

The following example shows how to configure the system mtu 2000 bytes.

Switch(config)#system mtu 2000