S3400 Web Configuration Manual

Maipu Communication Technology Co., Ltd
No. 16, Jiuxing Avenue
Hi-tech Park
Chengdu, Sichuan Province
People's Republic of China - 610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85148948, 85148139
URL: http:// www.maipu.com
Email: overseas@maipu.com

All rights reserved. Printed in the People's Republic of China.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without the prior written consent of Maipu Communication Technology Co., Ltd.

Maipu makes no representations or warranties with respect to this document contents and specifically disclaims any implied warranties of merchantability or fitness for any specific purpose. Further, Maipu reserves the right to revise this document and to make changes from time to time in its content without being obligated to notify any person of such revisions or changes.

Maipu values and appreciates comments you may have concerning our products or this document. Please address comments to:

Maipu Communication Technology Co., Ltd
No. 16, Jiuxing Avenue
Hi-tech Park
Chengdu, Sichuan Province
People's Republic of China - 610041
Tel: (86) 28-85148850, 85148041
Fax: (86) 28-85148948, 85148139
URL: http:// www.maipu.com
Email: overseas@maipu.com

All other products or services mentioned herein may be registered trademarks, trademarks, or service marks of their respective manufacturers, companies, or organizations.

Maipu Feedback Form

Your opinion helps us improve the quality of our product documentation and offer better services. Please fax your comments and suggestions to (86) 28-85148948, 85148139 or email to overseas@maipu.com.

<table>
<tr><td>Document Title</td><td colspan="4">S3400 WEB CONFIGURATION MANUAL</td></tr>
<tr><td>Product Version</td><td colspan="2"></td><td>Document Revision Number</td><td>1.0</td></tr>
<tr><td rowspan="3">Evaluate this document</td><td colspan="4">Presentation:
(Introductions, procedures, illustrations, completeness, arrangement, appearance)
☐ Good ☐ Fair ☐ Average ☐ Poor</td></tr>
<tr><td colspan="4">Accessibility:
(Contents, index, headings, numbering)
☐ Good ☐ Fair ☐ Average ☐ Poor</td></tr>
<tr><td colspan="4">Editorial:
(Language, vocabulary, readability, clarity, technical accuracy, content)
☐ Good ☐ Fair ☐ Average ☐ Poor</td></tr>
<tr><td>Your suggestions to improve the document</td><td colspan="4">Please check suggestions to improve this document:
☐ Improve introduction ☐ Make more concise
☐ Improve Contents ☐ Add more step-by-step procedures/tutorials
☐ Improve arrangement ☐ Add more technical information
☐ Include images ☐ Make it less technical
☐ Add more detail ☐ Improve index</td></tr>
<tr><td colspan="5">If you wish to be contacted, complete the following:</td></tr>
<tr><td>Name</td><td colspan="2"></td><td>Company</td><td></td></tr>
<tr><td>Postcode</td><td colspan="2"></td><td>Address</td><td></td></tr>
<tr><td>Telephone</td><td colspan="2"></td><td>E-mail</td><td></td></tr>
</table>

Contents

Preparations **8**
Login 8
Product Information **10**
Switch Port Configuration **12**
VLAN Configuration **41**
Default VLAN (PVID) of Port 41
Paging 42
Port-Based VLAN 42
Add VLAN 43
Edit VLAN 43
Overview 44
Introduction to MAC-VLAN 44
Add MAC-VLAN 44
Overview 45
Introduction to IP Subnet VLAN 45
Add IP Subnet VLAN 45
Overview 45
Introduction to Protocol VLAN 46
Add Protocol VLAN 46
Configure Protocol Profile 46
Overview 47
Introduction to Vlan dot1q tunnel 48
Q-IN-Q Configuration 49
Introduction to L2 protocol control 50
Configure Special Multicast MAC for Replacing Destination MAC of L2 Protocol Packet 51
L2 Protocol Control Configuration 52
ACL Configuration **53**
Add Rule 54
Delete 54
Create One IP Standard Access List 54
Bind Time Range 55
Bind Action Group 55
Configure IP Extended Access List 56

Create One Rule 56
Delete 56
Create One IP Extended Access List 57
Bind Object 58
Create One Rule 58
Delete 59
Create 59
Bind Object 59
Create One Rule 60
Delete 60
Create 60
Create One Rule 62
Delete 62
Create 62
Edit 63
Delete 64
Create 64
Delete 66
Apply 67
QoS Configuration 68
Priority Mapping 68
Edit 69
Delete 70
Queue Scheduling Mode 71
Edit 72
Delete 73
Drop Mode 74
Edit 75
Delete 76
Rate Limitation 76
Edit 77
Delete 78
Port Flow Shaping 79
Edit 80
Delete 81
Port Queue Flow Shaping 82
Edit 82
Delete 83
OAM Configuration 85
CFM Configuration 85
Overview 85
Maintenance Domain Configuration 86

CFM Port Configuration 89
OAM Basic Configurations 90
Port OAM Enabling Configuration 90
Port OAM Event Log Configuration 92
Port OAM Detection Packet Configuration 94
Port OAM Link Monitoring Configuration 96
OAM Status Display 101
OAM Remote Loopback Test 103
ELMI Configuration 106
E-LMI Protocol Configuration on PE 106
E-LMI Protocol Configuration on CE 109
EVC-UNI Configuration 109
Edit 110
Create New UNI 111
Delete 111
EVC Information 112
View Details 113
Anti-Attack Detection Configuration 114
Overview 114
Pseudo-source Address 114
Attack Detection 115
LAND Attack Detection 115
ICMP flood Attack Detection 115
SYN flood Attack Detection 116
Smurf Attack Detection 117
Fraggle Attack Detection 117
Scan Detection 118
Introduction to Scan Detection 118
Scan Detection Configuration 119
Static Route Configuration 120
Overview 120
Introduction to Static Route 120
Configure Static Route 121
DNS Configuration 122
Overview 122
DNS Server Configuration 122
System Management 123
Overview 123
Basic Information Configuration 123
NTP Configuration 123

Administrator Configuration 125
Device Software Upgrade 126
Configuration File Management 126
Log Management 127
Save Configuration 128
Overview 128

Preparations

Overview

The chapter describes the preparations for the WEB configuration of MyPower S3400 series switch.

📖 Note

The browser that supports the web configuration described in the chapter is Internet Explorer 6.0 or above.

Login

The web management system of the gateway supports two kinds of users, including administrator and common users. The MyPower S3400 series switch described in the manual does not have default user name or password, so you need to telnet to the gateway and configure login user in shell so that the web management system can be used normally. The following are the shell commands for configuring users.

Configure administrator:

MyPower S3400#configure terminal //enter into the configuration mode

MyPower S3400(config)#user admin privilege 15 password 0 admin //configure the administrator with user name as admin, priority as 15, and password as admin. 15 is the highest priority.

Configure common users:

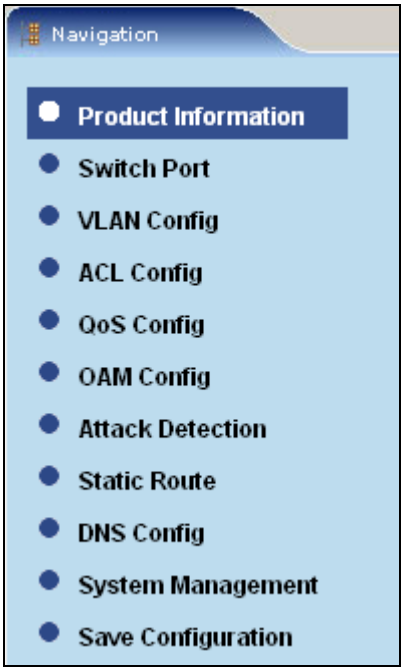
MyPower S3400#configure terminal // enter into the configuration mode

MyPower S3400(config)#user guest privilege 0 password 0 guest //configure the user with user name as guest, priority as 0, and password as guest. 0 is the lowest priority.

The administrator and common user correspond to different management authorities.

The administrator authorities include switch port configuration, VLAN configuration, ACL configuration, QoS configuration, OAM configuration, anti-attack detection configuration, DNS configuration, system management, and save configuration.

The corresponding function navigation is as follows:



The authorities of the common user include switch port configuration, VLAN configuration, anti-attack detection configuration, DNS configuration, system management, and save configuration.

The corresponding function navigation is as follows:

Product Information

Overview

The chapter describes the features and version information of MyPower S3400 series switch.

Features

MyPower S3400 series switch provides telecom-level Ethernet access switches for operators. It supports next generation L2 and L3 features and meets the requirements of customers for QoS, OAM, VPN, Multi-service and Protection.

S3400 can help customers develop IPTV, VoIP, VPN, wireless access and TDMoIP services. The high integrated platform design meets the requirement of the customer that a box provides rich physical interface and software features to reduce the total cost (TCO) and operating expenses (OpEx).

MyPower S3400 is the first in the world to adopt dual power supply, high integrated E1/T1 interface, standard PoE, and optical-electric Ethernet access on the access device. The operators adopt it to be deployed in 2G/3G base station for developing multi-service access (wireless, VPN, and mobile) and completing the reconstruction from TDM to IP.

S3400 has the following features:

Multi-service Ethernet switch with highest integrity

First to support dual power supply on access-level Ethernet device

Supports perfect OAM protocol

Supports VPN services defined by MEF

50ms Ethernet service protection

Supports QinQ and selective QinQ

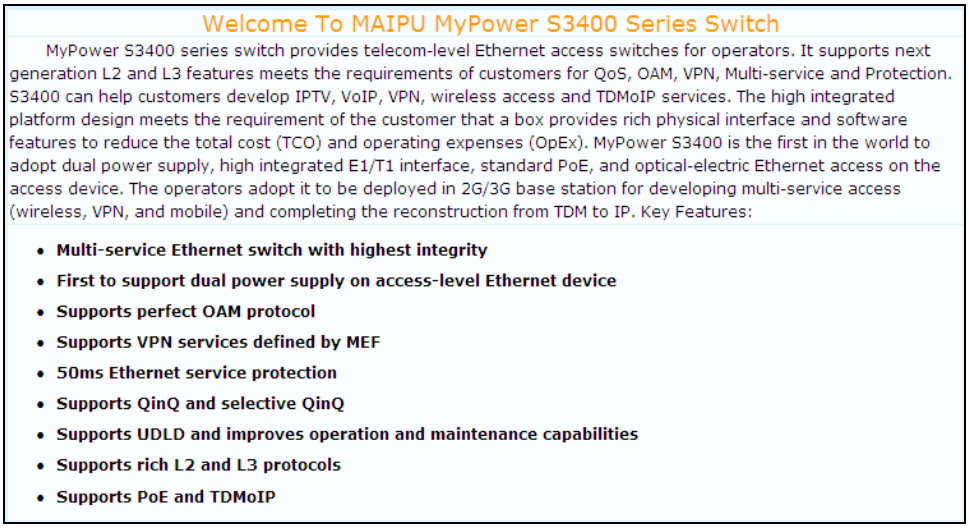
Supports UDLD and improves operation and maintenance capabilities

Supports rich L2 and L3 protocols

Supports PoE and TDMoIP

You can view via

, as follows:



Welcome To MAIPU MyPower S3400 Series Switch

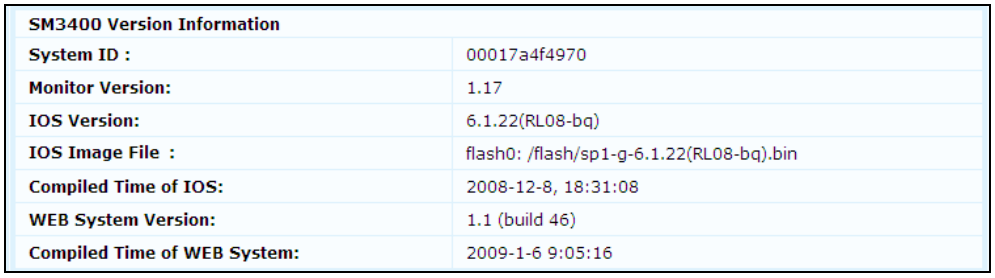
MyPower S3400 series switch provides telecom-level Ethernet access switches for operators. It supports next generation L2 and L3 features meets the requirements of customers for QoS, OAM, VPN, Multi-service and Protection. S3400 can help customers develop IPTV, VoIP, VPN, wireless access and TDMoIP services. The high integrated platform design meets the requirement of the customer that a box provides rich physical interface and software features to reduce the total cost (TCO) and operating expenses (OpEx). MyPower S3400 is the first in the world to adopt dual power supply, high integrated E1/T1 interface, standard PoE, and optical-electric Ethernet access on the access device. The operators adopt it to be deployed in 2G/3G base station for developing multi-service access (wireless, VPN, and mobile) and completing the reconstruction from TDM to IP. Key Features:

- **Multi-service Ethernet switch with highest integrity**
- **First to support dual power supply on access-level Ethernet device**
- **Supports perfect OAM protocol**
- **Supports VPN services defined by MEF**
- **50ms Ethernet service protection**
- **Supports QinQ and selective QinQ**
- **Supports UDLD and improves operation and maintenance capabilities**
- **Supports rich L2 and L3 protocols**
- **Supports PoE and TDMoIP**

System Version Information

You can view the current system version information via

, as follows:



SM3400 Version Information	
System ID :	00017a4f4970
Monitor Version:	1.17
IOS Version:	6.1.22(RL08-bq)
IOS Image File :	flash0: /flash/sp1-g-6.1.22(RL08-bq).bin
Compiled Time of IOS:	2008-12-8, 18:31:08
WEB System Version:	1.1 (build 46)
Compiled Time of WEB System:	2009-1-6 9:05:16

Switch Port Configuration

Basic Attribute Configuration

This section describes the configuration information of the port.

Port	Description	Status	Link	Set Speed	Act Speed	Set Duplex	Act Duplex	Set Flow Control	Act Flow Control	Mdix	Mtu	Link Delay	Pvid	Edit
0/0		enabled	up	auto	100	auto	full	off	off	auto	1728	0	1	
0/1		enabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	1	
0/2		enabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	1	
0/3		enabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	1	
0/4		disabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	3	
0/5		disabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	5	
0/6		enabled	up	auto	100	auto	full	off	off	auto	1728	0	1	
0/7		disabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	1	
0/8		disabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	1	
0/9		disabled	down	auto	unkown	auto	unkown	off	off	auto	1728	0	1	

Port: The numbers of all ports in the switch;

Description: The port description information for easy memory. You can configure the description information for one port. For example, one port is distributed to Company A and you can configure the description information as “company A”. The description information comprises up to 240 characters and there can be blanks between the characters. By default, the port does not have description information;

Status: Port status. When the value is enabled, it indicates that the port is enabled; when the value is disabled, it indicates that the port is disabled and cannot enter into the normal working state. The default value is enabled.

Link: The physical status of the port. By default, after the port is connected, the light is on and the link status is UP; when the port is not connected, the link status is down.

Set speed: The management speed of the port, including “10”, “100”, “1000”, and “auto”. Unit is M. “auto” means “auto-negotiation”;

Act speed: The actual speed of the port, including “10”, “100”, “1000”, and “auto”. Unit is M. “auto” means “auto-negotiation”;

Set duplex: The management duplex status of the port, including “auto”, “full”, and “half”. “auto” means “auto-negotiation”; “full” means “full-duplex”; “half” means “half-duplex”;

Act duplex: The actual duplex status of the port, including “auto”, “full”, and “half”. “auto” means “auto-negotiation”; “full” means “full-duplex”; “half” means “half-duplex”;

Set flow control: The management flow control of the port. “on” means to enable the port flow control; “off” means to disable the port flow control;

Act flow control: The actual flow control of the port. “on” means to enable the port flow control; “off” means to disable the port flow control. The default value is “off”.

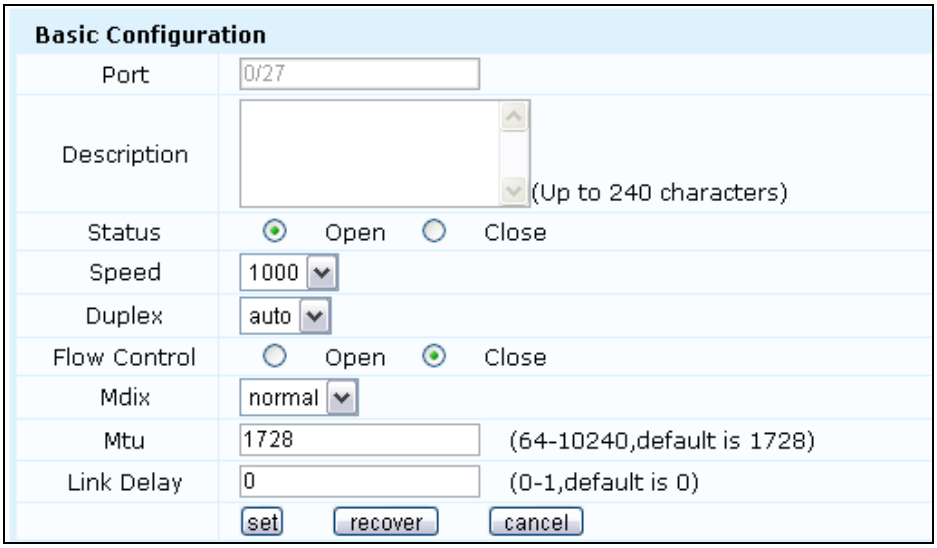
Mdix: The signal sending mode of the port. “normal” means that lines 1 and 2 are used for sending and line 3 and 6 are used for receiving; “cross” means that lines 1 and 2 are used for receiving and lines 3 and 6 are used for sending; “auto” means to select normal or cross automatically. The default value is auto.

Mtu: The MTU of the port. MTU is checked only when being input. The MTU is not checked when being output. If the length of the frame received by the port exceeds the set MTU, the frame is discarded. The unit is byte. It is required the configured value must be multiples of four bytes. Otherwise, it is cut down to the multiples of four. For example, the configured value is 1501 bytes, the system adjusts it to be 1500 bytes. The default value is 1728.

Link delay: The status delay time of the port. The default value is 0.

Pvid: The ID of the VLAN to which the port belongs. The default value is 1.

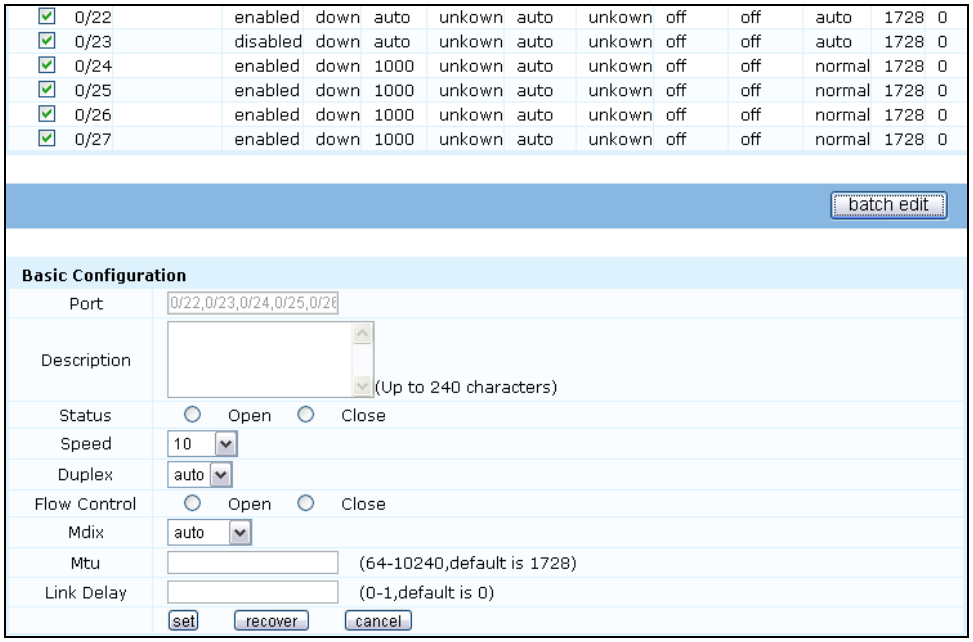
Edit: Click the icon of one port and you can configure the port.



Click **recover** to recover the port to the factory status.

📖 Note

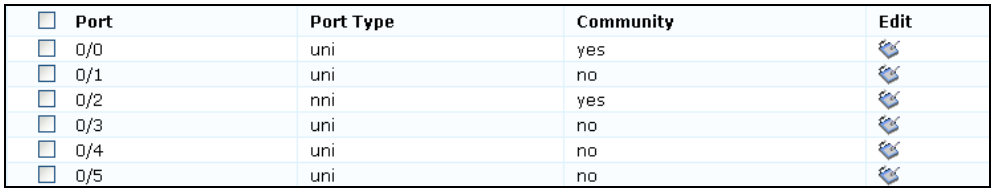
It is required that the configured value must be the multiple of four bytes. For example, the configured value is 1501 bytes, and the system adjusts it to be 1500 bytes.



Tick the check box before the port number, click batch edit and you can edit the ports in batches.

Port Type Configuration

This section describes the configuration information about the port type.



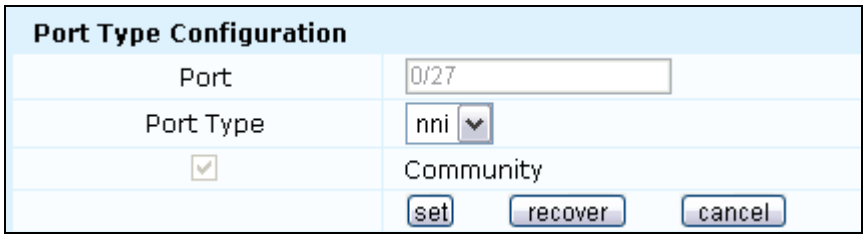
Port: The numbers of all ports in the switch;

Port type: The UNI/NNI attribute of the port. Each physical port of the switch has UNI/NNI attribute. By default, all 10M/100M ports are set as UNI ports and the other ports are set as NNI ports. You can also modify the UNI/NNI attribute of each port via configuration.

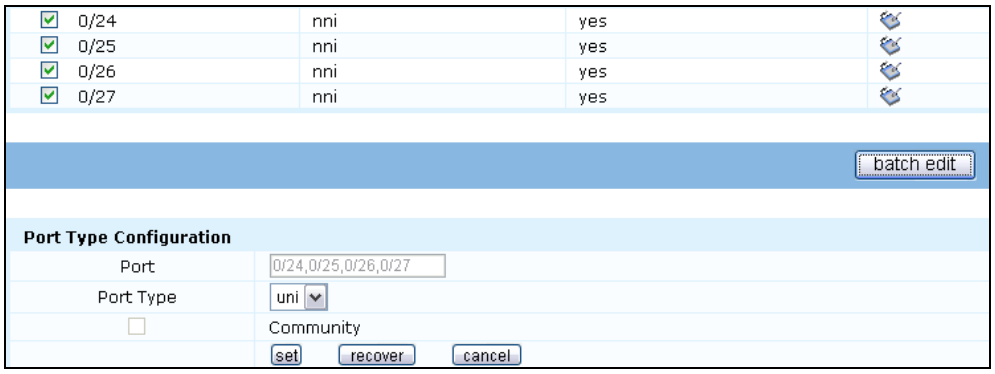
Communication with other UNI port: By default, the UNI port is shutdown and the UNI ports cannot communicate with each other, but UNI and NNI ports can communicate with each other; NNI ports can also communicate with each other. You can make some UNI ports can

communicate with each other via configuration. “yes” means that the port can communicate with other UNI port; “no” means that the port cannot communicate with other UNI port.

Edit: Click the icon of one port and you can configure the port.



Click **recover** to recover the port to the factory status.



Tick the check box before the port number, click **batch edit** and you can edit the ports in batches.

Port Storm Control

This section describes the configuration information about the port storm control.

Port	Unicast	Threshold	Broadcast	Threshold	Multicast	Threshold	Action Over Threshold	Edit
0/0	disabled		disabled		disabled		none	
0/1	disabled		disabled		disabled		none	
0/2	disabled		disabled		disabled		none	
0/3	disabled		disabled		disabled		none	
0/4	disabled		disabled		disabled		none	
0/5	disabled		disabled		disabled		trap	
0/6	disabled		disabled		disabled		none	
0/7	disabled		disabled		disabled		trap	
0/8	disabled		disabled		disabled		trap	
0/9	disabled		disabled		disabled		none	
0/10	disabled		disabled		disabled		trap	
0/11	disabled		disabled		disabled		none	
0/12	disabled		disabled		disabled		none	
0/13	disabled		disabled		disabled		none	
0/14	disabled		disabled		disabled		none	
0/15	disabled		disabled		disabled		none	
0/16	disabled		disabled		disabled		none	
0/17	disabled		disabled		disabled		none	
0/18	disabled		disabled		disabled		none	

Port: The numbers of all ports in the switch;

Unicast: The unknown unicast storm information of the port. “disabled” means that no unknown unicast storm information is configured; “bps” means to configure the storm control for bps (bits per second); “pps” means to configure the storm control for pps(packets per second). The default value is “disabled”.

Threshold(kbps): The unknown unicast storm threshold of the port. The unit of pps is kpps and the value range is 0-2000000; the unit of bps is kbps, the granularity is 64kbps, and the value range is 64-8000000, that is, 64kbps to 8G.

Broadcast: The broadcast storm information of the port. “disabled” means that no broadcast storm information is configured; “bps” means to configure the storm control for bps (bits per second); “pps” means to configure the storm control for pps(packets per second). The default value is “disabled”.

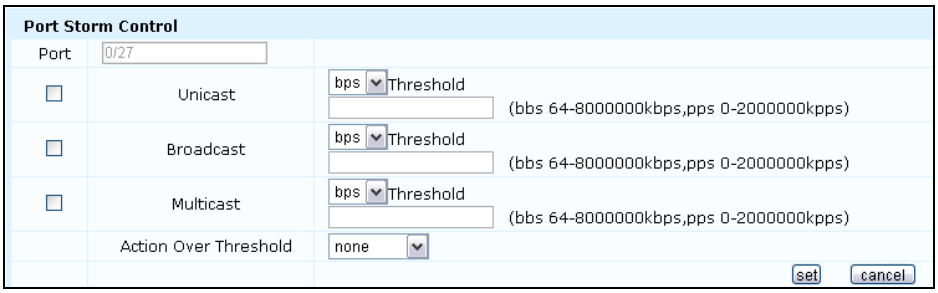
Threshold(kbps): The broadcast storm threshold of the port. The unit of pps is kpps and the value range is 0-2000000; the unit of bps is kbps, the granularity is 64kbps, and the value range is 64-8000000, that is, 64kbps to 8G.

Multicast: The unknown multicast storm information of the port; “disabled” means that no unknown multicast storm information is configured; “bps” means to configure the storm control for bps (bits per second); “pps” means to configure the storm control for pps(packets per second). The default value is “disabled”.

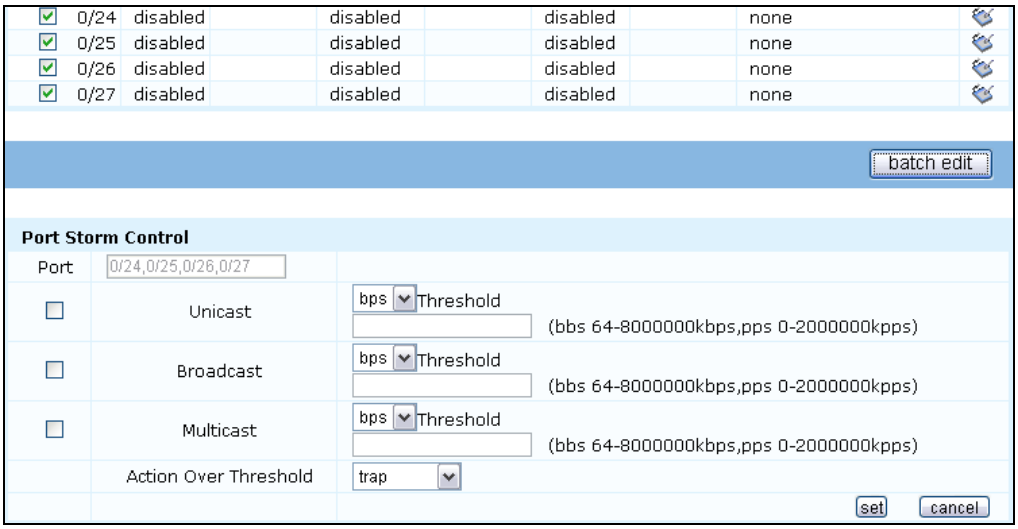
Threshold(kbps): The unknown multicast storm threshold of the port. The unit of pps is kpps and the value range is 0-2000000; the unit of bps is kbps, the granularity is 64kbps, and the value range is 64-8000000, that is, 64kbps to 8G.

Action Over Threshold: The action executed after storm suppression. “shutdown” means to shut down the port; “trap” means to send TRAP alarms; “none” means no storm control action. The default value is “none”.

Edit: Click the icon of one port and you can configure the port.

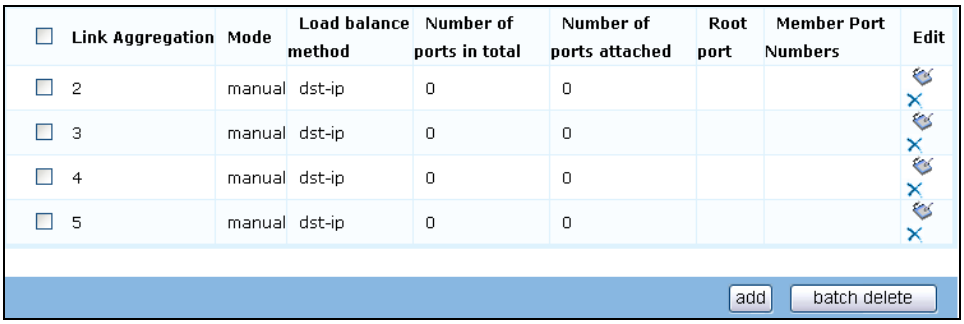


Tick the check box before the port number, click **batch edit** and you can edit the ports in batches.



Link Aggregation Configuration

This section describes the configuration information about the link aggregation.



Link Aggregation: The name of the link aggregation group;

Mode: The aggregation mode of the link aggregation. “manual” means the manual aggregation mode; “lacp” means the protocol aggregation mode.

Load balance method: The load balance algorithm of the link aggregation. “dst-ip” means the load balance algorithm based on destination IP address; “dst-mac” means the load balance algorithm based on destination MAC address; “src-dst-ip” means the load balance algorithm based on source and destination IP address; “src-dst-mac” means the load balance algorithm based on source and destination MAC address; “src-ip” means the load balance algorithm based on source IP address; “src-mac” means the load balance algorithm based on source MAC address; The default value is src-mac.

Number of ports in total: The total number of ports in the aggregation group;

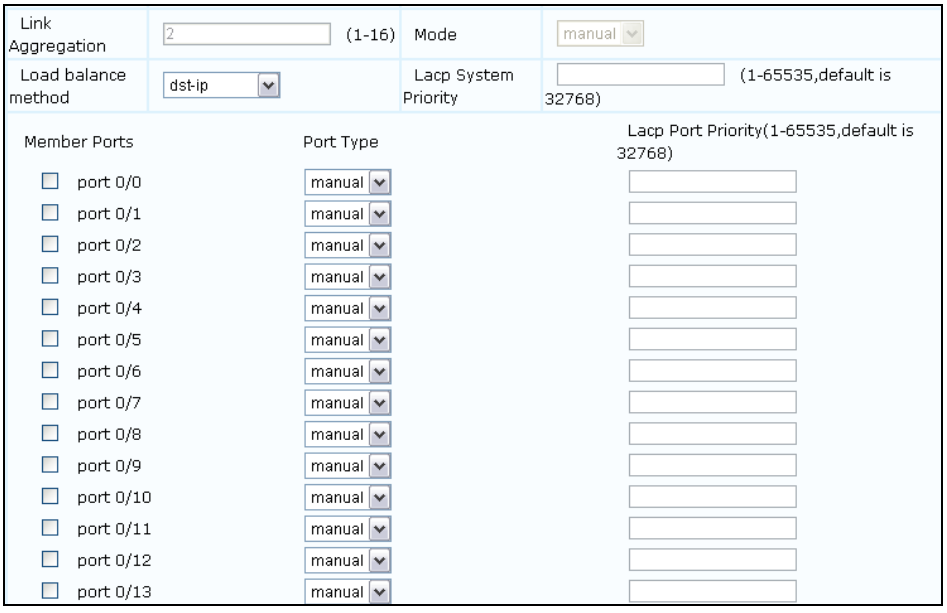
Number of ports attached: The number of the ports that are aggregated in the aggregation group;

Root port: The root port of the aggregation group;

Member port numbers: The numbers of the member ports in the aggregation group;

Edit: Click the icon of one aggregation group and you can configure the aggregation group. Click the icon of one aggregation group and you can delete the aggregation group.

Click the icon of one aggregation group to edit it.



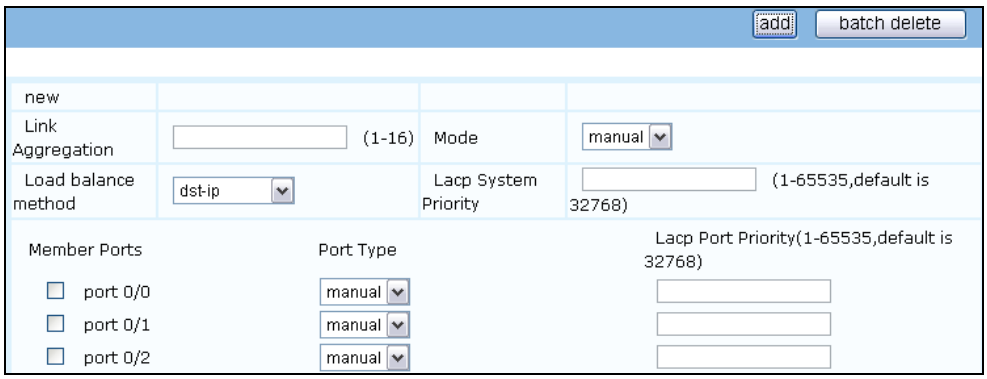
Note

For example, in aggregation group 1, the member ports are 0/11, 0/16, and 0/17. When clicking **Edit**, the check boxes before port 0/11, port 0/16, and port 0/17 in the member port list are selected. When the aggregation

mode is manual, the port types of the member ports can only be manual; when the aggregation mode is lacp, the port types of the member ports are active and passive.

When clicking the ✕ icon of one aggregation group to delete the aggregation group, click **Yes** to delete the record or click **Cancel** and the aggregation group is not deleted.

Add: Click **add** and you can perform the adding operation.



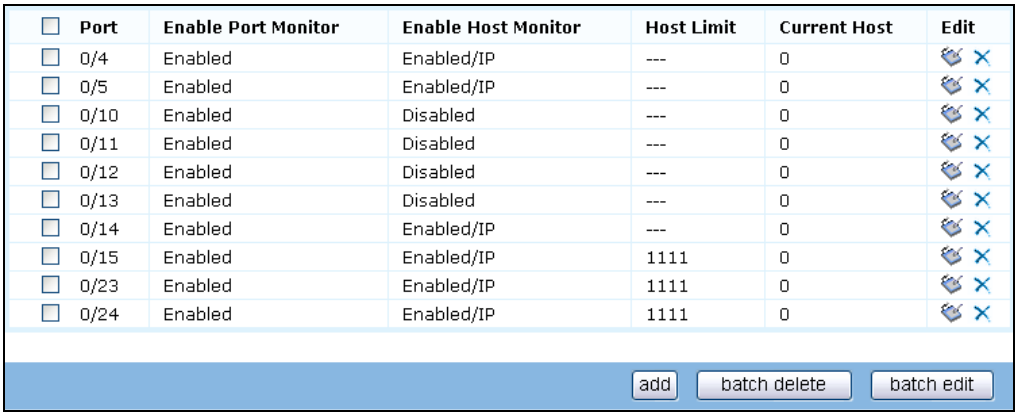
batch delete: Click **batch delete** and you can delete the aggregation groups in batches.

📖 Note

To delete the link aggregations in batches, you should first tick the check boxes before the aggregation groups. When the prompt box appears, click **Yes** to delete the selected records or click **Cancel** and the selected records are not deleted.

Port Monitoring Configuration

This section describes the configuration information about the port monitoring.



Port	Enable Port Monitor	Enable Host Monitor	Host Limit	Current Host	Edit
0/4	Enabled	Enabled/IP	---	0	
0/5	Enabled	Enabled/IP	---	0	
0/10	Enabled	Disabled	---	0	
0/11	Enabled	Disabled	---	0	
0/12	Enabled	Disabled	---	0	
0/13	Enabled	Disabled	---	0	
0/14	Enabled	Enabled/IP	---	0	
0/15	Enabled	Enabled/IP	1111	0	
0/23	Enabled	Enabled/IP	1111	0	
0/24	Enabled	Enabled/IP	1111	0	

add batch delete batch edit

Port: The number of the port that is configured with port monitoring in the switch;

Enable port monitor: Whether to enable the port-level monitoring. “Enabled” means to enable the port-level monitoring; “Disabled” means to disable the port-level monitoring. The default value is Disabled;

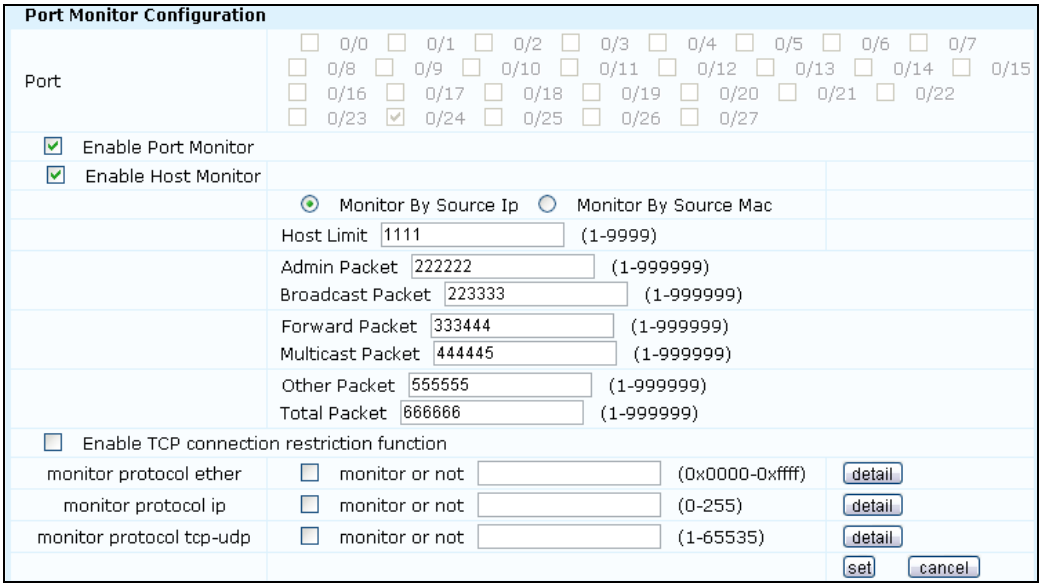
Enable Host Monitor: Whether to enable host-level monitoring. “Enabled/IP” means to monitor by source IP; “Enabled/MAC” means to monitor by source MAC; “Disabled” means not to monitor. The default value is Disabled.

Host Limit: The maximum number of the hosts that are monitored;

Current Host: The number of the current hosts;

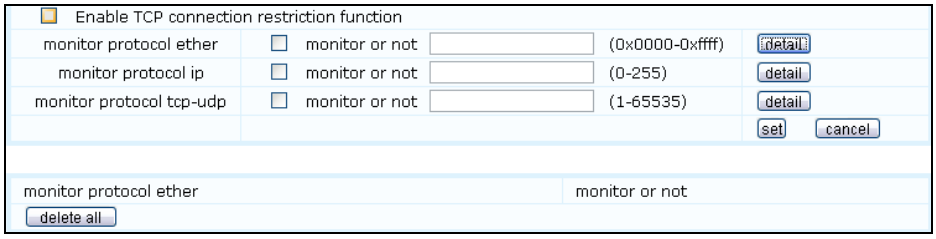
Edit: Click the icon of one port and you can configure the port. Click the icon of one port and you can delete the port.

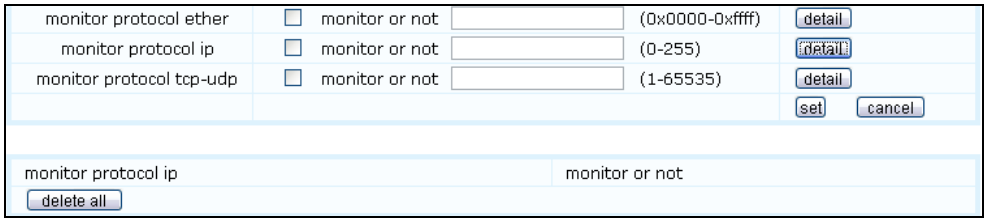
Click the icon of one port to edit it.

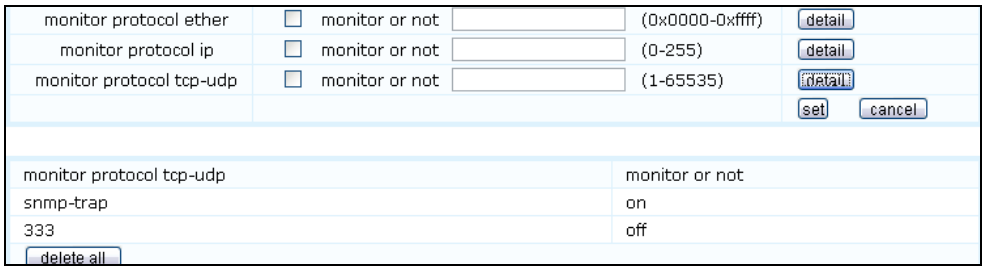


Note

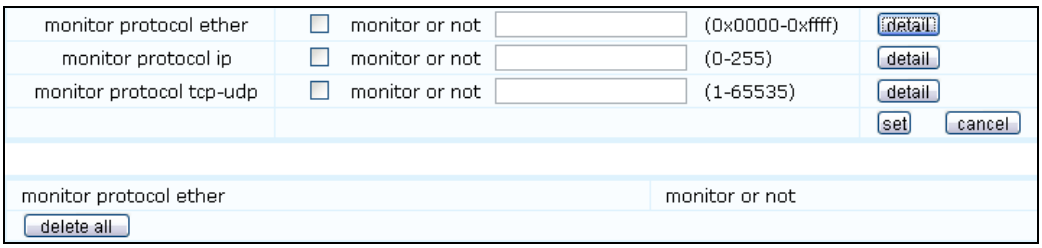
After clicking the edit icon, you can set the parameters of the port monitoring. The host monitoring can be enabled only after the port monitoring is enabled and you should select **Monitor by source IP** or **Monitor by source MAC**. You can view the details by clicking the **detail** button of **monitor protocol ether**, **monitor protocol ip** and **monitor protocol tcp/udp**.



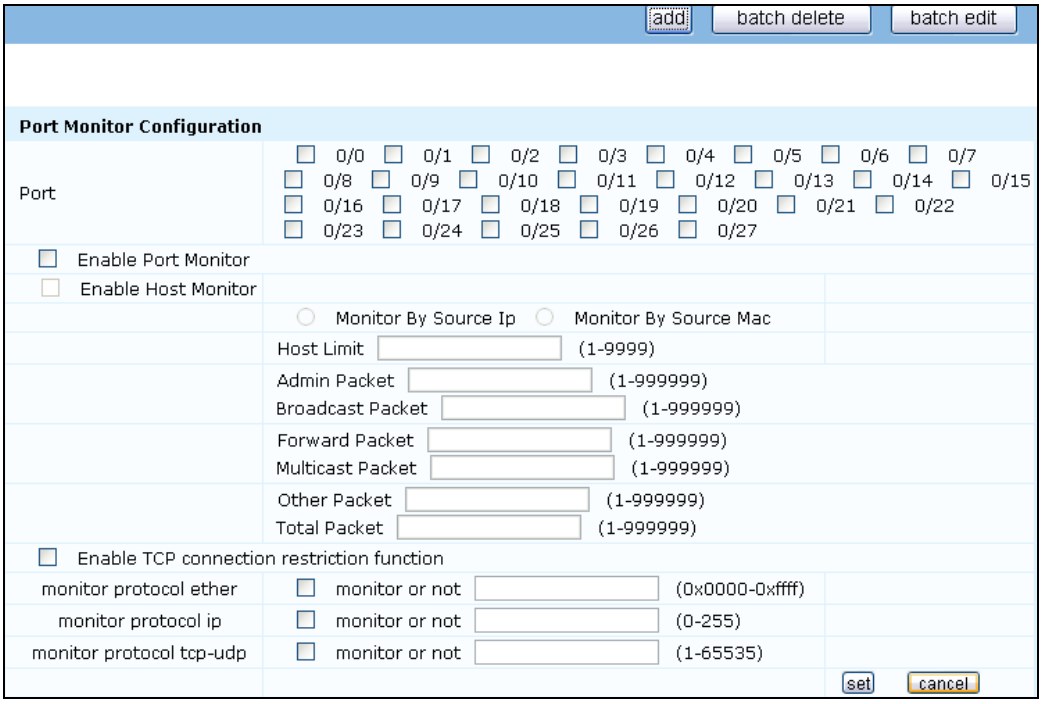




After clicking the **delete all** button of **monitor protocol ether**, **monitor protocol ip** and **monitor protocol tcp/udp**, a confirming box appears and click **Yes** to delete all information or click **Cancel**. After deleting, the result is as follows:



Add: Click **add** and you can perform the adding operation.

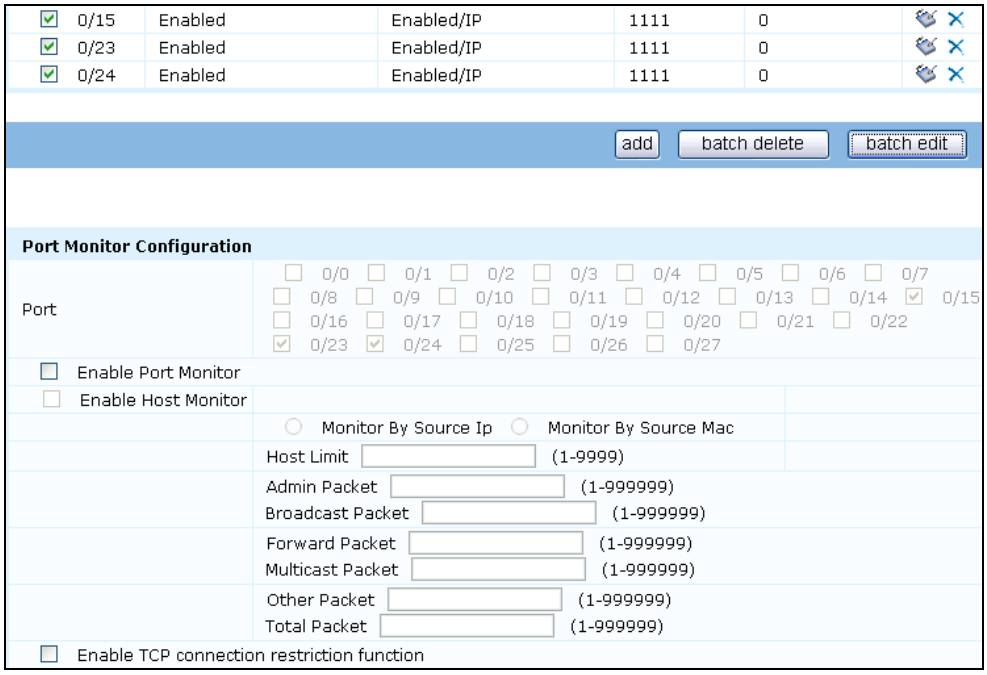


📖 Note

Tick the check boxes in the port list and you can add port monitoring in batches. For example, after selecting ports 0/0, 0/1, and 0/2, click **set** and then the ports 0/0, 0/1, and 0/2 are configured with port monitoring. When adding new port monitoring, the details of **monitor protocol ether**, **monitor protocol ip** and **monitor protocol tcp/udp** are unavailable.

Batch delete: Click **batch delete** and you can delete the port monitoring in batches.

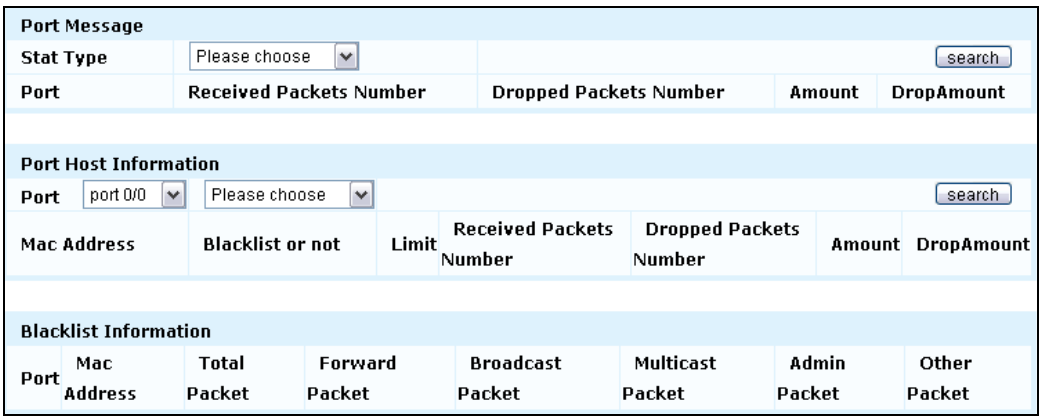
Batch edit: Click **batch edit** and you can edit the port monitoring in batches.



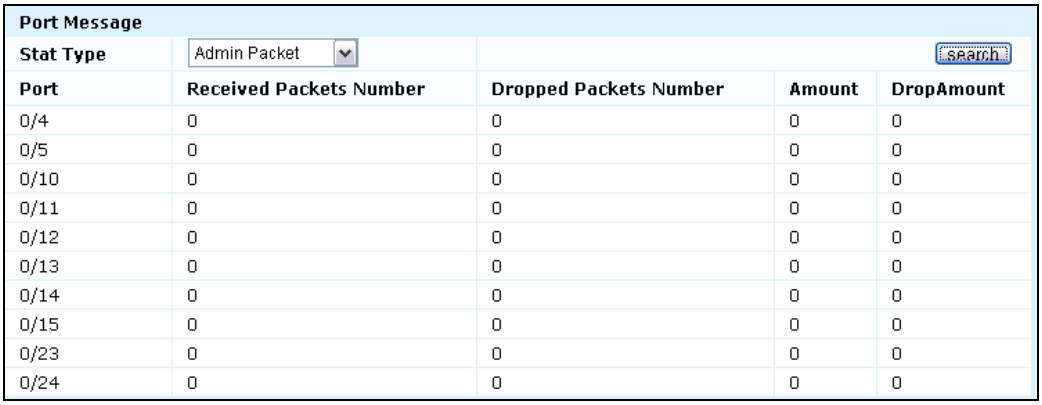
As shown in the above figure, the selected ports are displayed in the selected form in the lower port list.

Port Monitoring Statistics

This section describes the statistics information about the port monitoring.



Port Packets: You can select administration packets, broadcast packets, forwarding packets, multicast packets, other packets or all packets from the **Stat Type** drop-down list. After selecting one, click **Search** and the details about the select packet type are displayed as follows.



Port: the number of the port on which the port monitoring is enabled;

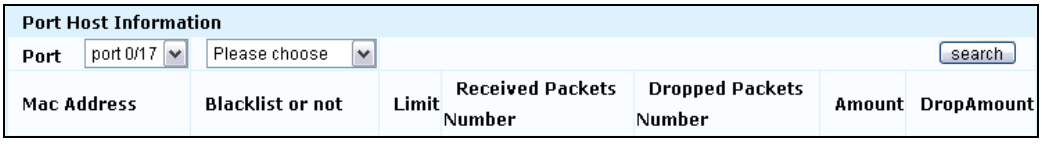
Received Packets Number: the number of the packets received by the port;

Dropped Packet Number: the number of the packets dropped by the port;

Amount: The total number of the packets received by the port;

Drop Amount: The total number of the packets dropped by the port;

Port Host Information: the numbers of all physical ports in the switch. You can select administration packets, broadcast packets, forwarding packets, multicast packets, other packets or all packets from the drop-down list. After selecting one, click **Search** and the details about the select packet type are displayed as follows.



Mac Address: The MAC address of the host in each host;

Backlist or not: Whether the host is in the backlist;

Limit: The maximum limitation of the host;

Received Packets Number: the number of the packets received by the host;

Dropped Packet Number: the number of the packets dropped by the host;

Amount: The total number of the packets received by the host;

Drop Amount: The total number of the packets dropped by the host;

Backlist Information: Display the backlist to view the hosts that initiate the attack;

Blacklist Information							
Port	Mac Address	Total Packet	Forward Packet	Broadcast Packet	Multicast Packet	Admin Packet	Other Packet

802.1X Authentication Configuration

This section describes the configuration information of the port 802.1X authentication.

Port	Enable 802.1X Configuration	Max User Number	Current User	EAPOL Packet Transmission	Uplink Port	Port Multicast Trigger	Guest Vlan	EAP Relay	Reauthperiod	Timeout Quiet Period
0/2	enable	256	0	enable	11	enable		enable	600	60
0/3	enable	256	0	disable		disable		disable	600	60
0/4	enable	256	0	enable		disable		disable	600	60
0/20	enable	256	0	enable		disable		disable	600	60
0/21	enable	256	0	disable		disable		disable	600	60
0/22	enable	256	0	disable		disable		disable	600	60
0/23	enable	256	0	disable		disable		disable	600	60
3	enable	256	0	enable		enable		enable	600	60

add

Port: The number of the port configured with 8021X authentication;

Enable 8021X Configuration: “enable” means to enable 8021X; “disable” means to disable 8021X. The default value is disable;

Max User Number: the maximum number of users of the port. The default value is 256;

Current user: The number of the current users of the port;

EAPOL packet transmission: the EAPOL packet transparent transmission function of the port; “enable” means to enable the EAPOL packet transparent transmission; “disable” means to disable the EAPOL packet transparent transmission. The default value is disable.

Uplink port: the uplink port during EAPOL packet transparent transmission;

Port multicast trigger: the function of triggering multicast on the port; “enable” means to enable the function of triggering multicast on the port; “disable” means to disable the function of triggering multicast on the port. The default value is disable.

Guest Vlan: the guest vlan of the port;

EAP relay: the EAP mode of the port, including EAP relay or EAP termination. “enable” means to enable the EAP relay mode; “disable”

means to disable the EAP relay mode (enable the EAP termination mode). The default value is disable;

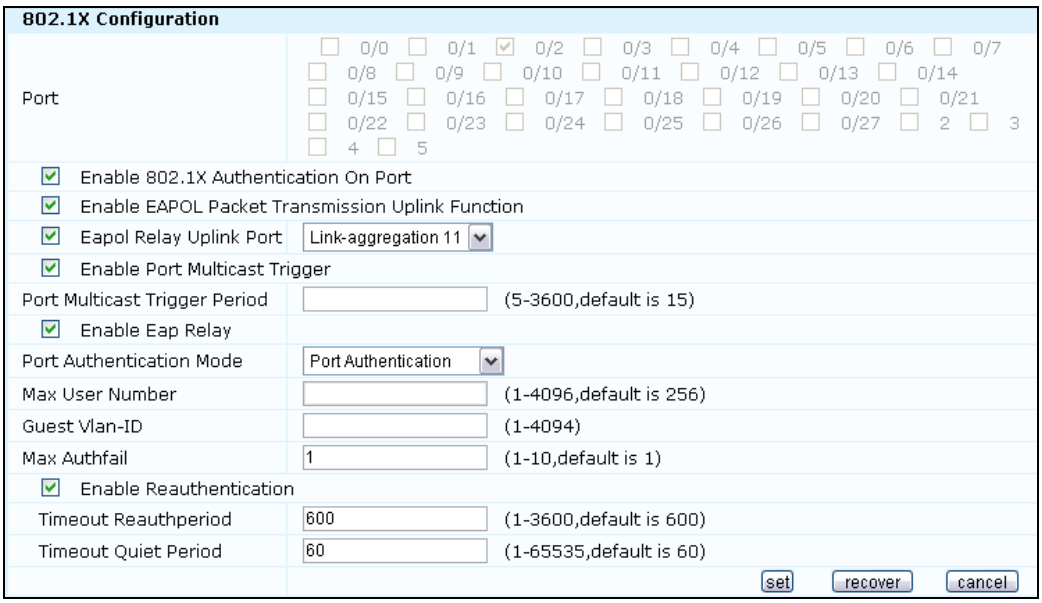
Reauthperiod: the re-authentication time of the port (second). When the re-authentication is enabled on the port, the re-authentication is performed during the period. The default value is 600.

Timeout Quiet Period: the punishment time of the port (second). When the successive failed authentication times of one reaches the upper threshold, the user cannot perform authentication during the punishment time. The default value is 60.

Max Authentication Failure Times: the maximum authentication failure times of the port. When the authentication failure times of one user reaches the upper threshold, the user can re-authenticate only after a certain time. The default value is one.

Port Authentication Mode: the 802.1X authentication mode of the port, including port-based authentication mode or user-based authentication mode. “portbased” means the authentication mode based on the port; “macbased” means the authentication mode based on the user. The default value is macbased.

Edit: Click of one port and you can edit the port.

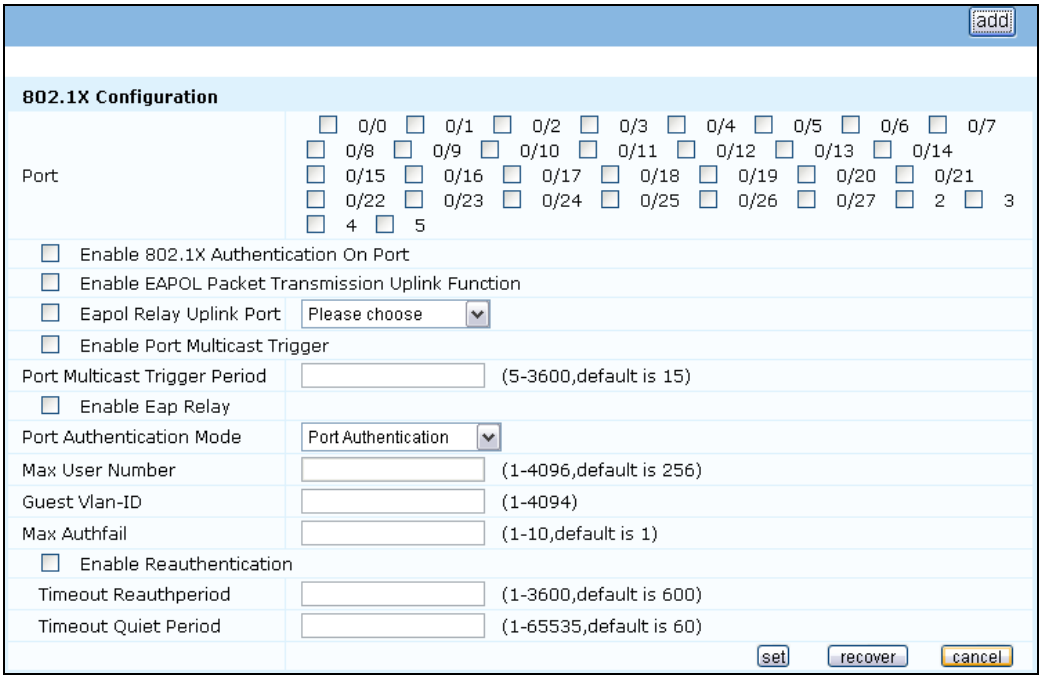


Note

For the port-based authentication mode, the maximum user number of the port does not take effect; for the user-based authentication mode, the configuration of guest vlan does not take effect.

Click **recover** to recover the port to the factory status.

Add: Click **add** and you can perform the adding operation.

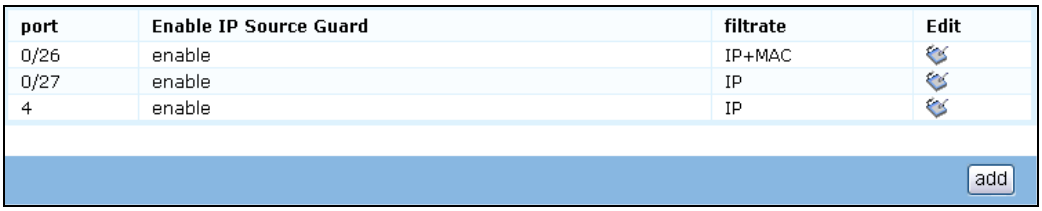


📖 Note

You can select multiple check boxes in the port list to perform batch operation.

IP Source Guard Configuration

This section describes the configuration information about IP Source Guard.

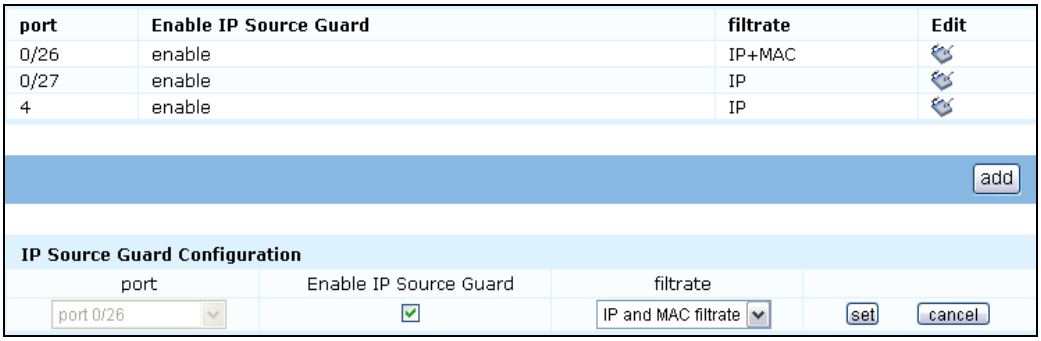


Port: The number of the port configured with IP Source Guard (including aggregation port number);

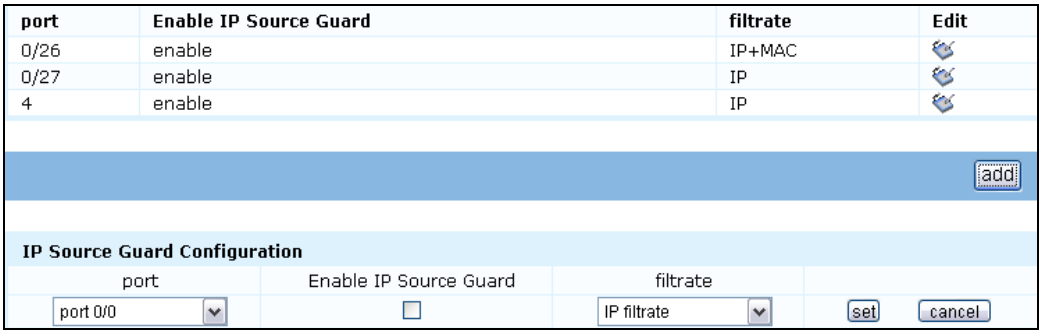
Enable IP Source Guard: "enable" means to enable the IP Source Guard function one the port;

Filtrate: "IP+MAC" means to enable the IP Source Guard function by the IP+MAC filtering mode; "IP" means to enable the IP Source Guard function by the IP filtering mode;

Edit: Click of one port and you can edit the port.

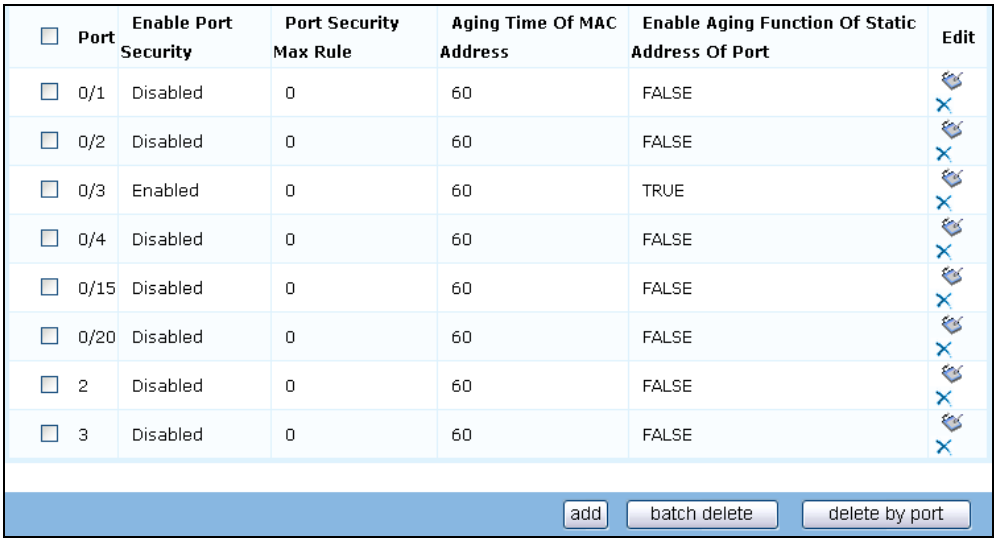


Add: Click **add** and you can perform the adding operation.



Port Security Configuration

This section describes the configuration information about the port security.



Port: The number of the port configured with the port security (including the aggregation port number);

Enable port security: the port security function. “Enabled” means to enable the port security; “Disabled” means to disable the port security. The default value is Disabled.

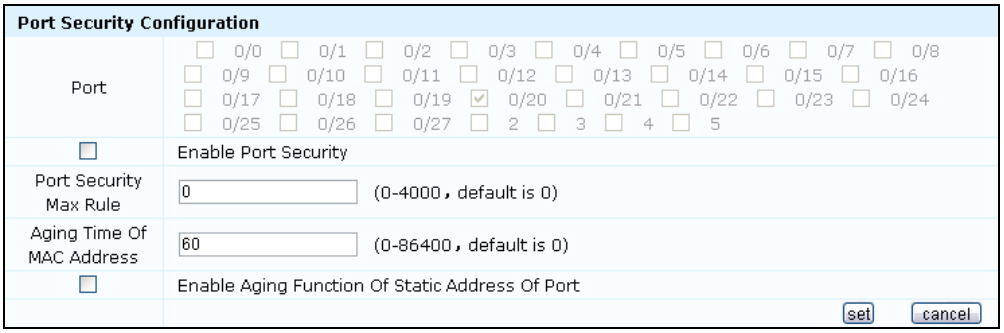
Port MAX Rule: the MAX rule of the port. The default value is 0;

Aging Time of MAC Address: the address aging time of the port; the default value is 0;

Enabling Aging Function of Static Address of Port: It is the aging function of the static address of the port; “TRUE” means to enable the aging function of the static address of the port; “FALSE” means to disable the aging time of the static address of the port. The default value is FALSE;

Edit: Click the icon of one port and you can edit the port. Click the icon of one port and you can delete the port.

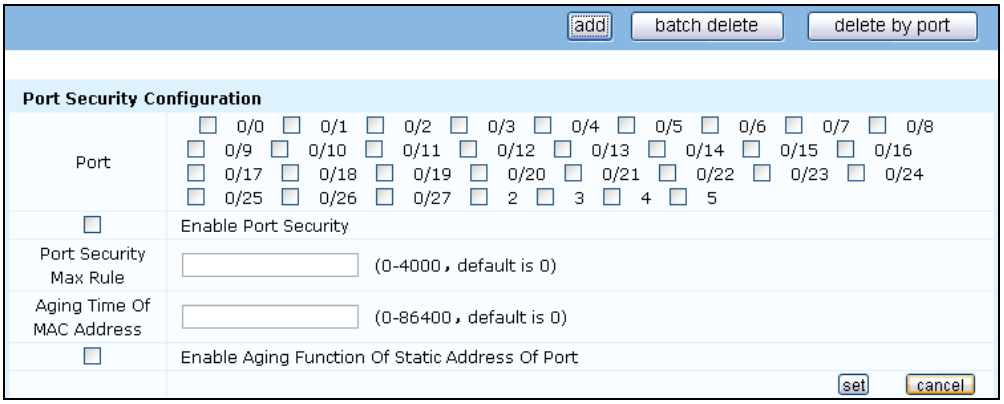
Click the icon of one port to edit it.



Click the icon of one port and you can delete the port.

You can tick the check boxes before the port numbers in the port list to perform the batch operation.

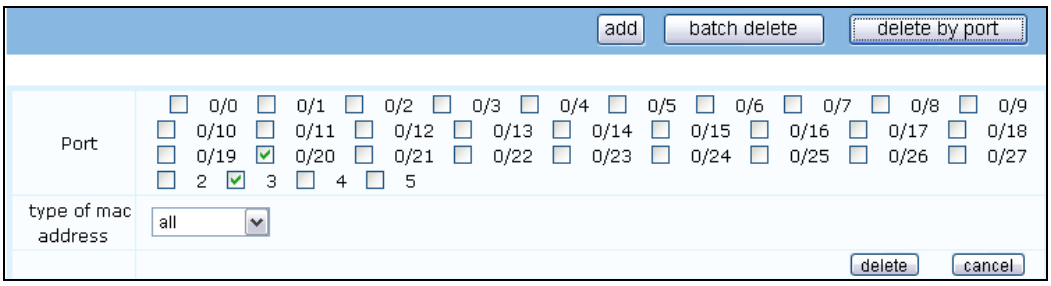
Add: Click **add** and you can perform the adding operation.



Note

You can tick multiple check boxes in the port list to perform the batch operation.

Delete Specified MAC of Port: Tick the check boxes in the port list and you can delete the specified MAC addresses of ports in batches;

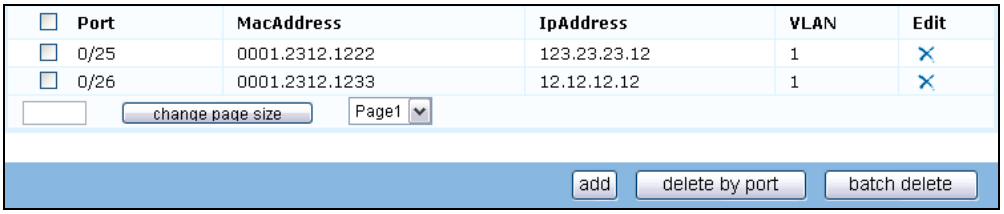


📖 Note

When **type of mac address** is **all**, it means to delete all MAC addresses; when **type of mac address** is **configured**, it means to delete all MAC address except for MAX rules; when **type of mac address** is **learned**, it means to delete the MAC addresses learned by MAX rules.

IP Binding Configuration

This section describes the configuration information about the IP binding.



Port: The number of the port configured with IP binding (including the aggregation port)

MAC Address: MAC address;

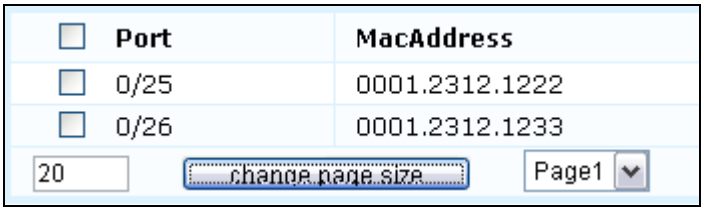
IpAddress: IP address

VLAN: VLAN ID;

Edit: You can click ✕ of one port to delete it.

📖 Note

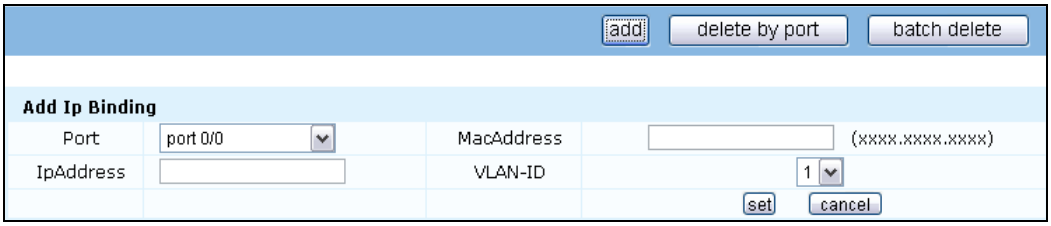
One port can be bound for several times, so the interface adopts the paging function for users to view. The interface can be paged as desired by adjusting the text box before **change page size**. For example, the interface has three pieces of information. If the user inputs one and then clicks **change page size**, the interface is displayed by three pages. If the user does not input, but clicks **change page size** directly, the interface is paged by the default 20, as follows.



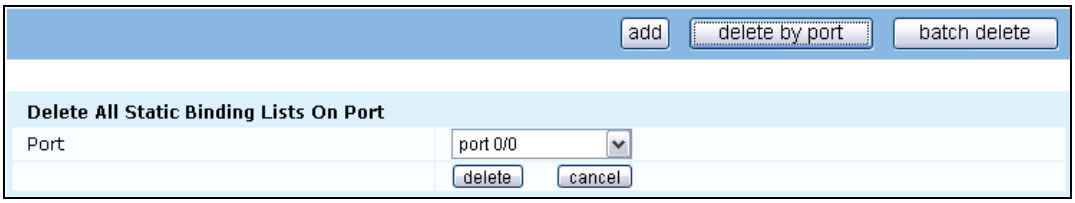
You can click ✕ of one port to delete it.

Batch delete: Tick the check boxes in the port list, click **batch delete** and you can perform the batch operation.

Add: Click **add** and you can perform the adding operation.

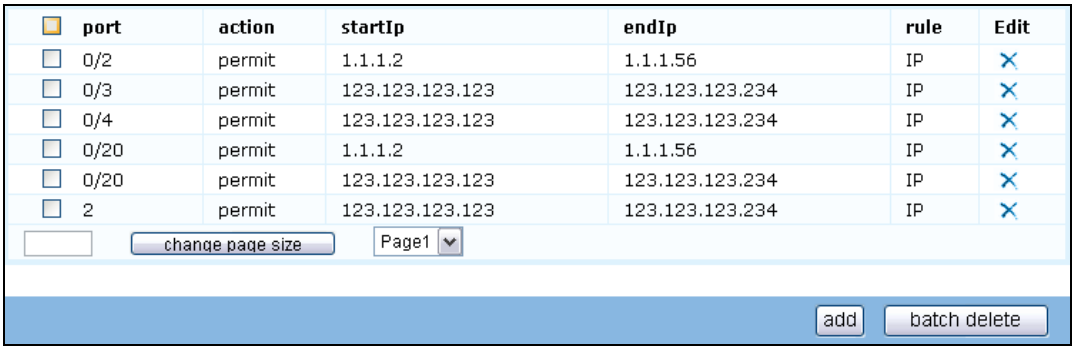


delete by port: click **delete by port** and you can delete all binding information on the port.



IP Rule Configuration

This section describes the configuration information about the IP rule.



Port: the number of the port configured with IP rule (including the aggregation port);

Action: the executed action of the rule. “permit” means that the executed action of the rule is permit; “deny” means that the executed action of the rule is deny.

Startip: The start IP address of the rule application;

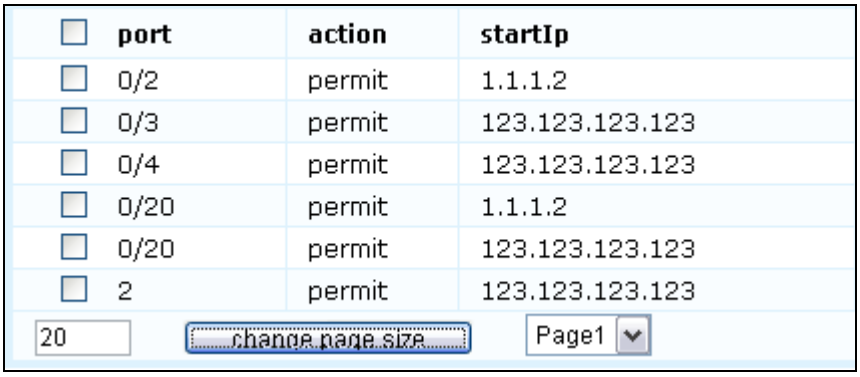
endIp: The end IP address of the rule application;

Rule: The IP rule;

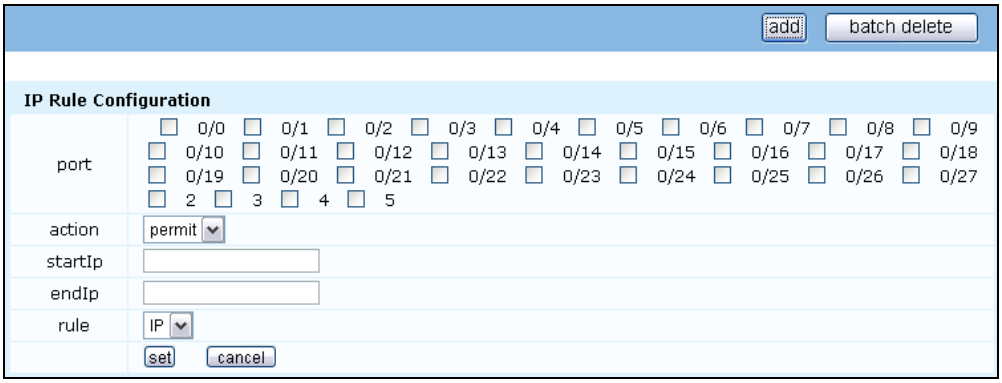
Edit: You can click ✕ of one port to delete it.

📖 Note

One port can be bound for several times, so the interface adopts the paging function for users to view. The interface can be paged as desired by adjusting the text box before **change page size**. For example, the interface has three pieces of information. If the user inputs one and then clicks **change page size**, the interface is displayed by three pages. If the user does not input, but clicks **change page size** directly, the interface is paged by the default 20, as follows.



Add: Click **add** and you can perform the adding operation.



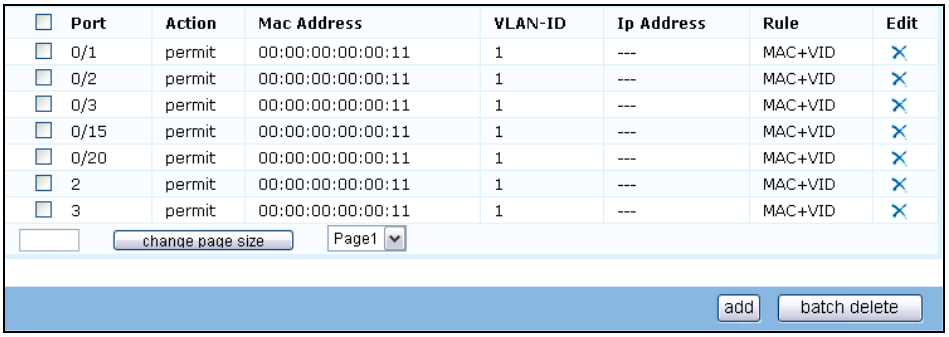
Note

Tick the check boxes in the port list and you can perform the batch operation.

Batch delete: Tick the check boxes in the port list, click **batch delete** and you can perform the batch operation.

MAC Rule Configuration

This section describes the configuration information about the MAC rule.



Port: the number of the port configured with MAC rule (including the aggregation port);

Action: the executed action of the rule. “permit” means that the executed action of the rule is permit; “deny” means that the executed action of the rule is deny.

MAC Address: the MAC address of the rule application;

VLAN-ID: the ID of the VLAN bound to the MAC address;

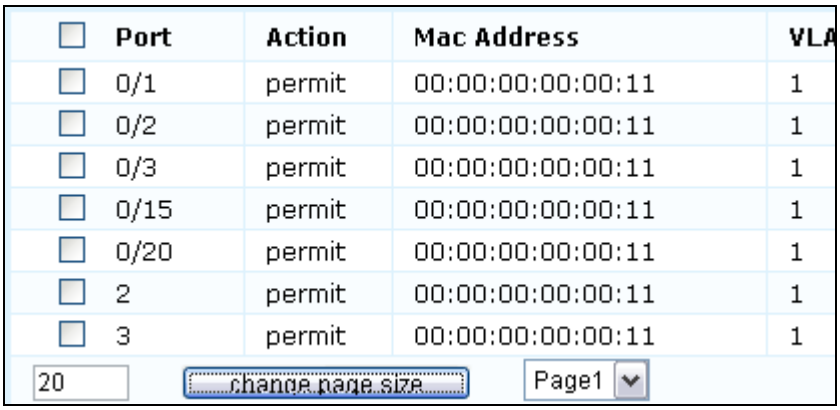
IP Address: the IP address;

Rule: “MAC+VID” means the MAC+VLAN binding rule; “MAC+IP” means the MAC+IP binding rule; “MAC” means the MAC binding rule;

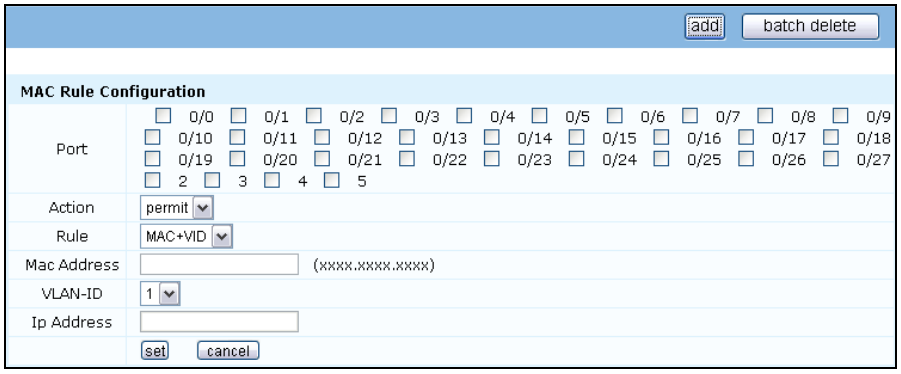
Edit: You can click ✕ of one port to delete it.

📖 Note

One port can be bound for several times, so the interface adopts the paging function for users to view. The interface can be paged as desired by adjusting the text box before **change page size**. For example, the interface has three pieces of information. If the user inputs one and then clicks **change page size**, the interface is displayed by three pages. If the user does not input, but clicks **change page size** directly, the interface is paged by the default 20, as follows.



Add: Click **add** and you can perform the adding operation.



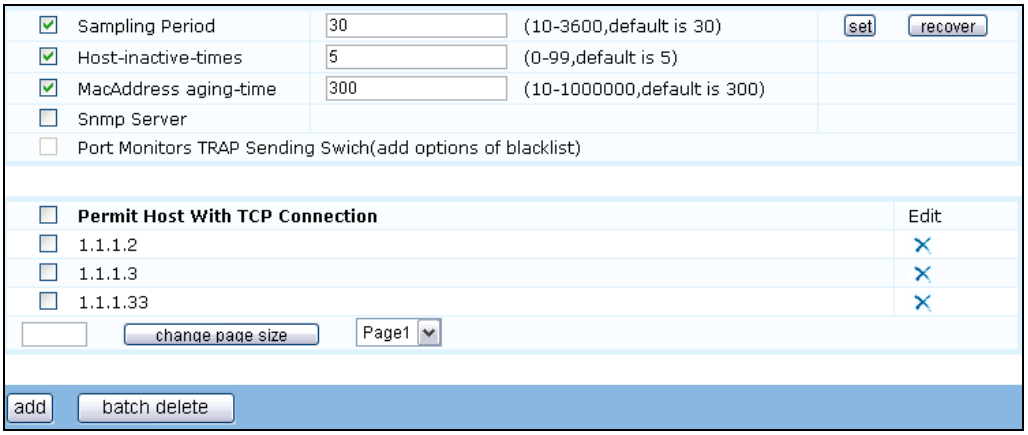
📖 Note

Tick the check boxes in the port list and you can perform the batch operation.

Batch delete: Tick the check boxes in the port list, click **batch delete** and you can perform the batch operation.

Global Parameter Configuration

This section describes the configuration information about the global parameters.



Sampling period: the sampling period of the port (second). After the port monitoring is enabled, the port monitoring function is used to measure the packets to CPU in each period. The default value is 30. Ticking the check box means to set the item;

Host-inactive-times: the aging time of the host (the unit is the sampling period). The default value is 5. Ticking the check box means to set the item;

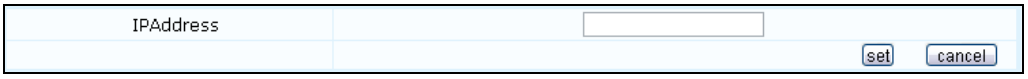
MacAddress aging-time: The aging time of the dynamic MAC address. The default value is 300. Ticking the check box means to configure the dynamic MAC address; no ticking the check box means to disable the aging function;

SNMP switch: Ticking the check box means to enable snmp-server; not ticking the check box means to disable the snmp-server;

Port Monitors TRAP Sending Switch (add options of backlist): snmp-server must be enabled for enabling the port monitoring TRAP sending switch;

Permit Host with TCP Connection: The list of the hosts that are permitted to set up TCP connection with the switch; the displayed information is the IP addresses of the hosts;

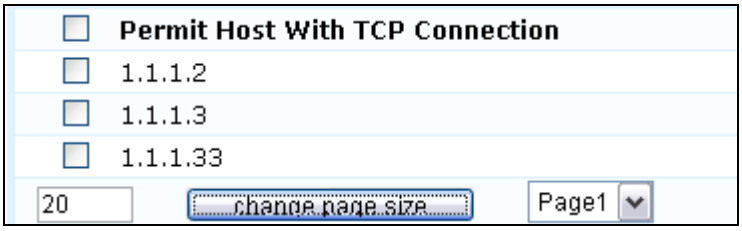
Add: Click **Add** and you can add a new TCP connection;



📖 Note

One port can be bound for several times, so the interface adopts the paging function for users to view. The interface can be paged as desired

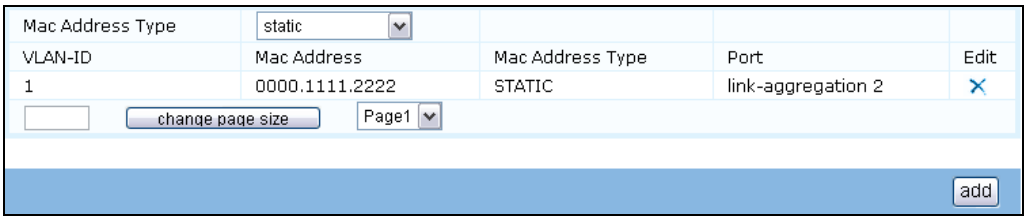
by adjusting the text box before **change page size**. For example, the interface has three pieces of information. If the user input one and then click **change page size**, the interface is displayed by three pages. If the user does not input, but clicks **change page size** directly, the interface is paged by the default 20, as follows.



Batch delete: Tick the check boxes in the port list, click **batch delete** and you can perform the batch operation.

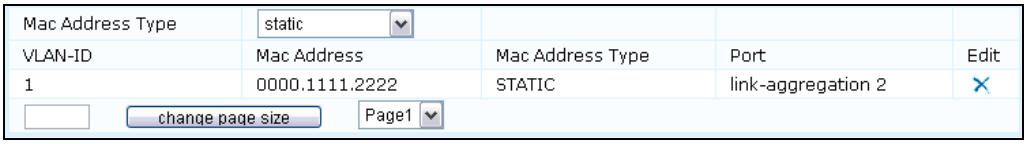
MAC Address Management

This section describes the information about the MAC address management.

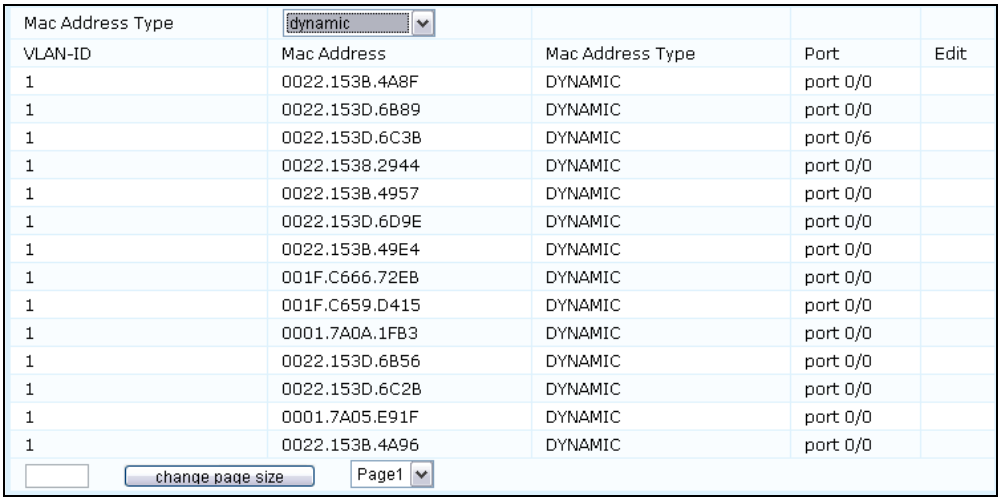


MAC Address Type: The options in the drop-down list are dynamic, static, drop, and all (without drop);

If **static** is selected, the displayed information is as follows:



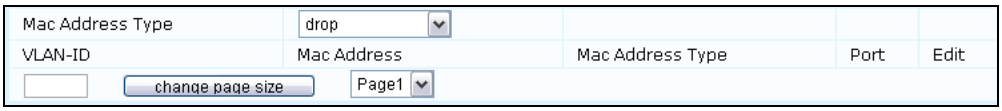
If **dynamic** is selected, the displayed information is as follows:



Mac Address Type	dynamic			
VLAN-ID	Mac Address	Mac Address Type	Port	Edit
1	0022.153B.4A8F	DYNAMIC	port 0/0	
1	0022.153D.6B89	DYNAMIC	port 0/0	
1	0022.153D.6C3B	DYNAMIC	port 0/6	
1	0022.1538.2944	DYNAMIC	port 0/0	
1	0022.153B.4957	DYNAMIC	port 0/0	
1	0022.153D.6D9E	DYNAMIC	port 0/0	
1	0022.153B.49E4	DYNAMIC	port 0/0	
1	001F.C666.72EB	DYNAMIC	port 0/0	
1	001F.C659.D415	DYNAMIC	port 0/0	
1	0001.7A0A.1FB3	DYNAMIC	port 0/0	
1	0022.153D.6B56	DYNAMIC	port 0/0	
1	0022.153D.6C2B	DYNAMIC	port 0/0	
1	0001.7A05.E91F	DYNAMIC	port 0/0	
1	0022.153B.4A96	DYNAMIC	port 0/0	

change page size Page1

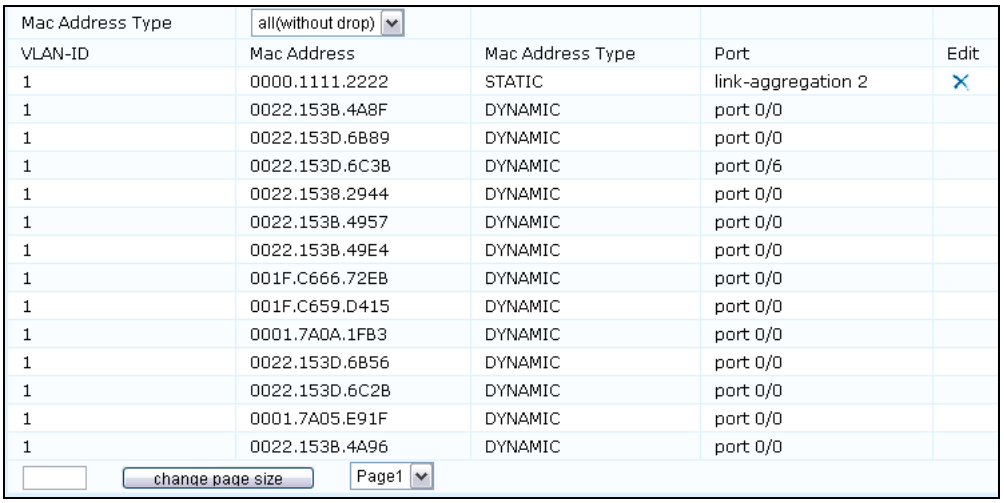
If **drop** is selected, the displayed information is as follows:



Mac Address Type	drop			
VLAN-ID	Mac Address	Mac Address Type	Port	Edit

change page size Page1

If **all (without drop)** is selected, the displayed information is as follows:



Mac Address Type	all(without drop)			
VLAN-ID	Mac Address	Mac Address Type	Port	Edit
1	0000.1111.2222	STATIC	link-aggregation 2	✕
1	0022.153B.4A8F	DYNAMIC	port 0/0	
1	0022.153D.6B89	DYNAMIC	port 0/0	
1	0022.153D.6C3B	DYNAMIC	port 0/6	
1	0022.1538.2944	DYNAMIC	port 0/0	
1	0022.153B.4957	DYNAMIC	port 0/0	
1	0022.153B.49E4	DYNAMIC	port 0/0	
1	001F.C666.72EB	DYNAMIC	port 0/0	
1	001F.C659.D415	DYNAMIC	port 0/0	
1	0001.7A0A.1FB3	DYNAMIC	port 0/0	
1	0022.153D.6B56	DYNAMIC	port 0/0	
1	0022.153D.6C2B	DYNAMIC	port 0/0	
1	0001.7A05.E91F	DYNAMIC	port 0/0	
1	0022.153B.4A96	DYNAMIC	port 0/0	

change page size Page1

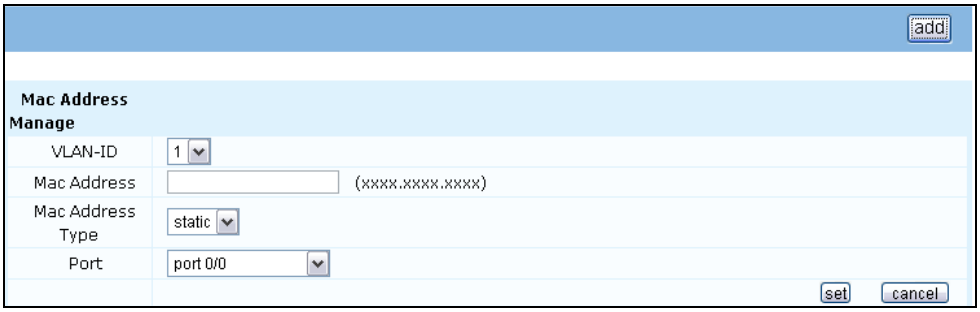
📖 Note

There are a lot of MAC addresses, so the interface adopts the paging function for users to view. The interface can be paged as desired by adjusting the text box before **change page size**. For example, the interface has three pieces of information. If the user inputs one and then clicks **change page size**, the interface is displayed by three pages. If the user does not input, but clicks **change page size** directly, the interface is paged by the default 20, as follows.

Mac Address Type	all(without drop)	
VLAN-ID	Mac Address	Mac Address
1	0000.1111.2222	STATIC
1	0022.153B.4A8F	DYNAMIC
1	0022.153D.6B89	DYNAMIC
1	0022.153D.6C3B	DYNAMIC
1	0022.1538.2944	DYNAMIC
1	0022.153B.4957	DYNAMIC
1	0022.153B.49E4	DYNAMIC
1	001F.C666.72EB	DYNAMIC
1	001F.C659.D415	DYNAMIC
1	0001.7A0A.1FB3	DYNAMIC
1	0022.153D.6B56	DYNAMIC
1	0022.153D.6C2B	DYNAMIC
1	0001.7A05.E91F	DYNAMIC
1	0022.153B.4A96	DYNAMIC
20	change page size	Page1

Edit: You can click ✕ of one port to delete it.

Add: Click **Add** and you can add a new MAC address. The MAC address type includes static and dynamic.



MAC Address Learning

This section describes the configuration information about MAC address learning.

Port	MAC Address Learning Account	Edit
0/0	not limit	
0/1	not limit	
0/2	not limit	
0/3	not limit	
0/4	not limit	
0/5	not limit	
0/6	not limit	
0/7	not limit	
0/8	not limit	
0/9	not limit	
0/10	not limit	
0/11	not limit	
0/12	not limit	
0/13	not limit	

Port: the number of the port configured with MAC address learning (including the aggregation port);

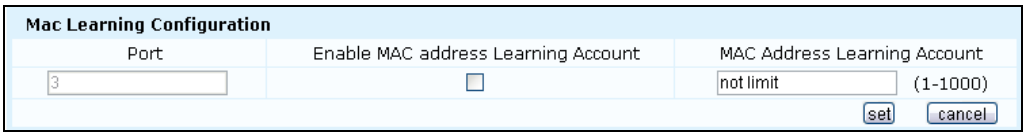
MAC Address Learning Account: The maximum number of MAC addresses learned by the port. By default, the number of the MAC addresses learned by the port is not limited, that is, set the maximum number of learned MAC addresses supported by hardware.

Caution

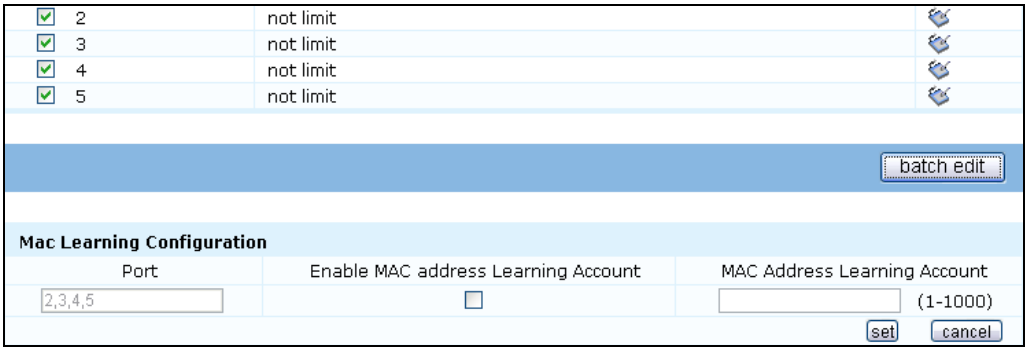
After canceling the limitation for the number of MAC addressed learned by the port, the number of MAC addresses learned by the port becomes the default value.

When the MAC address learning function is not enabled on the port, modifying the number of learned MAC addresses does not take effect.

Edit: Click of one port and you can edit it.

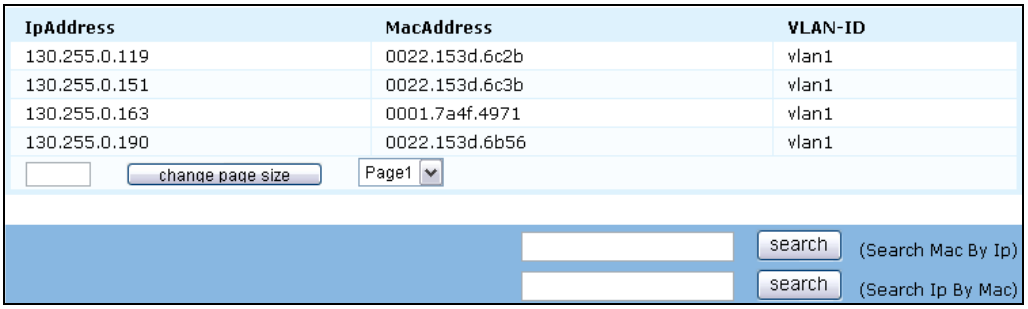


Batch edit: Click **batch edit** and you can perform the batch editing operation;



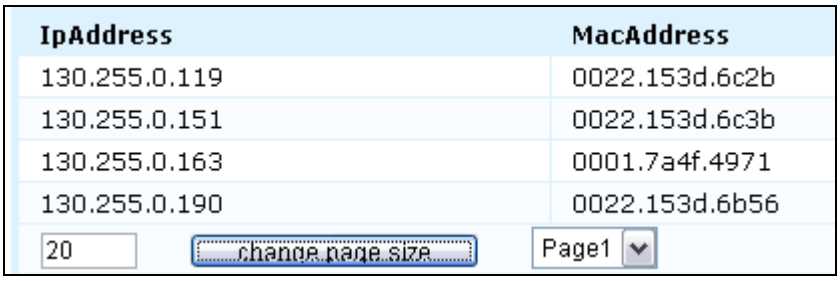
ARP Management

This section describes the ARP information.



📖 Note

There is lots of ARP to be displayed, so the interface adopts the paging function for users to view. The interface can be paged as desired by adjusting the text box before **change page size**. For example, the interface has three pieces of information. If the user inputs one and then clicks **change page size**, the interface is displayed by three pages. If the user does not input, but clicks **change page size** directly, the interface is paged by the default 20, as follows.



Search Mac by Ip: Input IP address in the text box before the **search** button, click **search** and then you can find the corresponding MAC addresses;

Search Ip by Mac: Input MAC address in the text box before the **search** button, click **search** and then you can find the corresponding IP addresses;

📖 Note

In the chapter, all physical ports in the port list are displayed in the form of 0/0, 0/1…0/27; the aggregation ports are displayed as 1, 2, 3…16.

VLAN Configuration

Overview

This chapter describes the VLAN configuration of MyPower S3400 series switch.

Port Mode

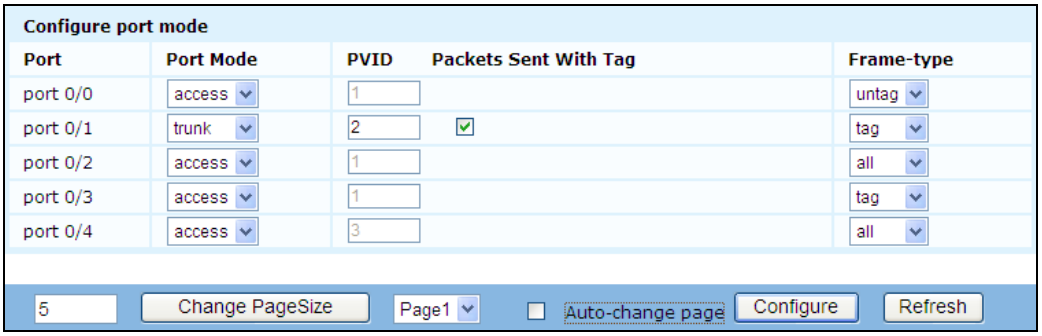
This section describes the configuration of the port mode.

Default VLAN (PVID) of Port

The packets without tag received by the port are divided to the default value. The default VLAN of the port is 1. The user can configure the default VLAN of the port as desired.

The default VLAN of the access port is the one to which it belongs, which cannot be configured.

Trunk port can Hybrid port can belong to several VLANs. The default VLAN can be configured.



Paging

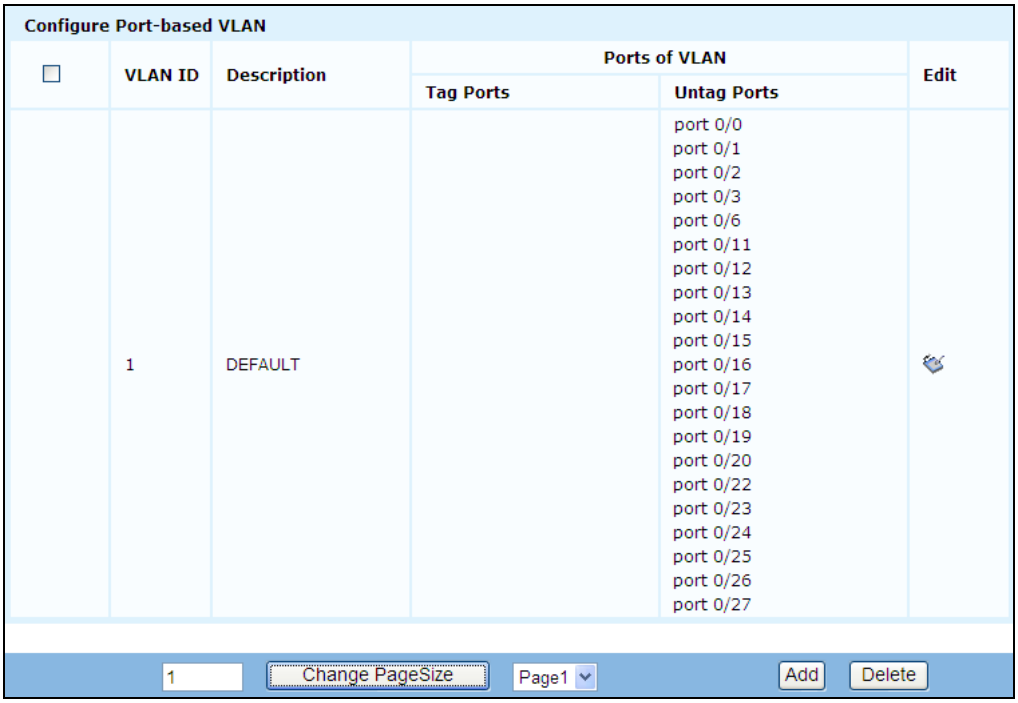
The system has the default value for the number of the records displayed in each page. You can input the desired number of the records displayed in each page in the text box of PageSize, and then click Change PageSize. When Auto-change page is selected, automatically turn to the next page (if it is the last page, turn to the home page) as long as the previous page is set successfully.

Basic VLAN Configuration

This section describes the port-based VLAN configuration.

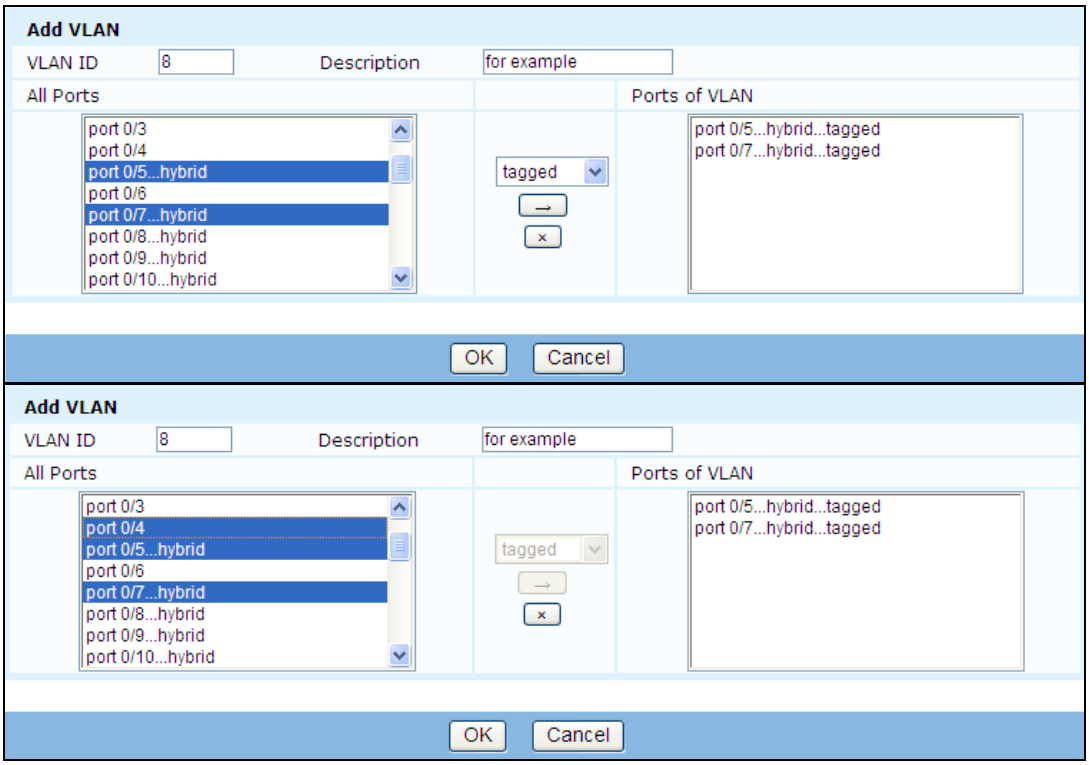
Port-Based VLAN

The port-based VLAN regards the port as one member added to the VLAN. The port can forward the packets of the VLAN.



Add VLAN

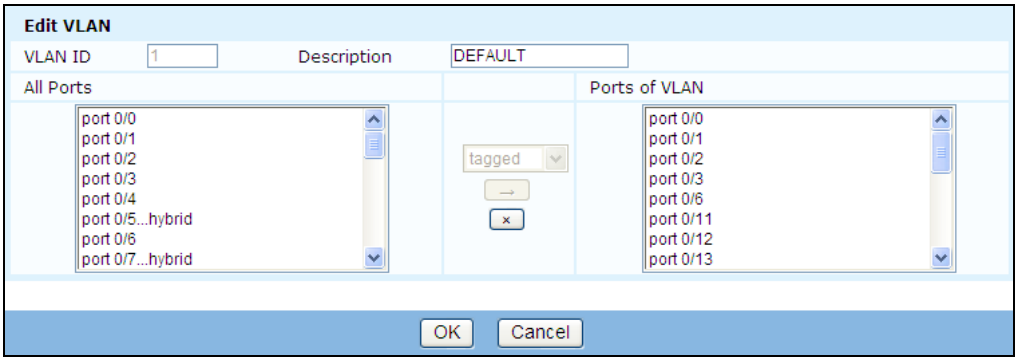
Click Add and you can add a new VLAN.



You can select multiple ports from the port list and click to add the selected ports to the member port list, but the types of the selected ports must be consistent (here, the classification standard is: hybrid mode/non-hybrid mode); click X and you can remove the ports from the member port list (multiple ports can be selected). At last, click OK to finish the VLAN configuration.

Edit VLAN

Click and you can edit the corresponding VLAN.



VLAN ID cannot be edited and the other parts are the same as the section of *Add VLAN*.

MAC-VLAN Configuration

Overview

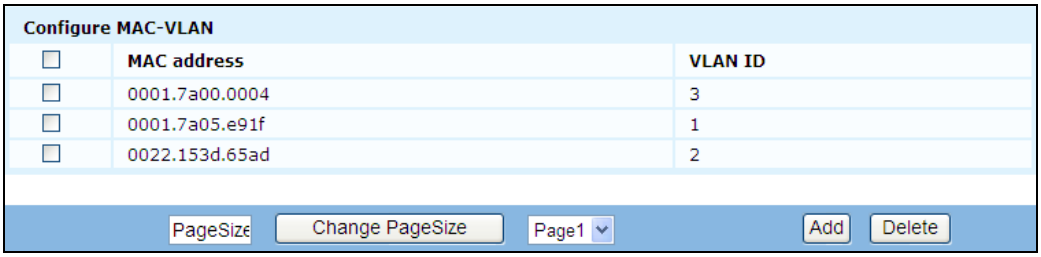
This section describes the MAC-based VLAN configuration in the port VLAN.

Introduction to MAC-VLAN

MAC-based VLAN is to divide VLAN ID to the packet according to the source MAC address of the untag (without tag) packet received by the port.

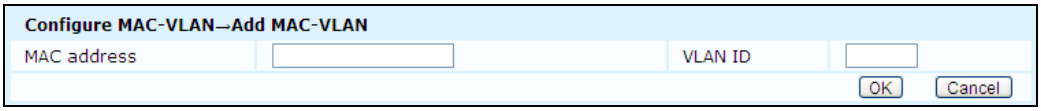
Process the untag packets received by the port as follows:

- If the source MAC address of the packet is consistent with the MAC address of the VLAN that is distributed based on MAC, the packet is distributed to the VLAN ID of the MAC VLAN.
- If the packet does not match the MAC address set by MAC VLAN, the packet is distributed to the default VLAN ID of the port.



Add MAC-VLAN

Click Add, and you can add new MAC-VLAN.



IP Subnet VLAN Configuration

Overview

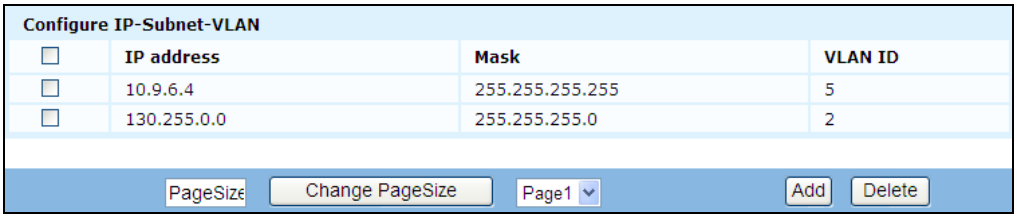
This section describes the IP subnet-based VLAN configuration in the port VLAN.

Introduction to IP Subnet VLAN

IP subnet-based VLAN is to divide VLAN ID to the packet according to the source IP address of the untag (without tag) packet received by the port.

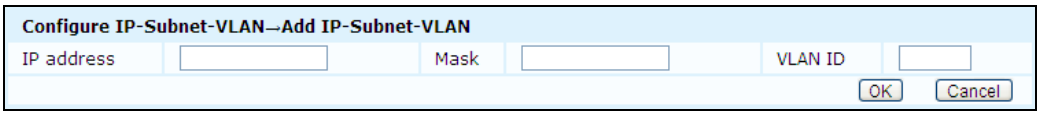
Process the untag packets received by the port as follows:

- If the source IP address of the packet is in the segment of IP subnet-based VLAN, the packet is distributed to the VLAN ID of the segment.
- If the packet is not in the segment of IP subnet VLAN, the packet is distributed to the default VLAN ID of the port.



Add IP Subnet VLAN

Click Add, and you can add new IP subnet VLAN.



Protocol VLAN Configuration

Overview

This section describes the protocol-based VLAN configuration in the port VLAN.

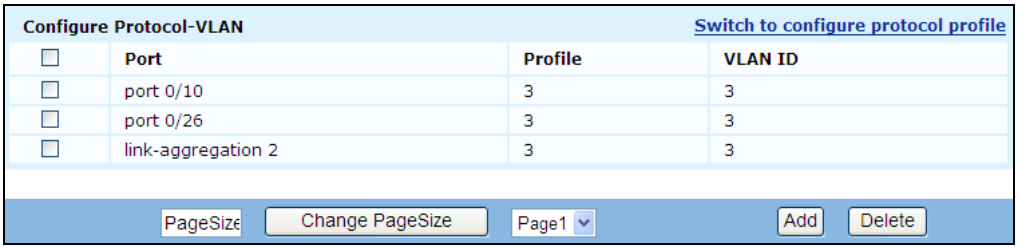
Introduction to Protocol VLAN

Protocol-based VLAN is to distribute VLAN ID to the packet according to the frame encapsulation format and protocol type of the untag packet (without tag) received by the port.

The protocol VLAN defines the protocol profile, which comprises the frame encapsulation and protocol type. One port can be configured with several protocol profiles. When the protocol VLAN is enabled on the port, the protocol profile is configured on the port.

The protocol VLAN processes the untag packet received by the port as follows:

- If the packet matches the protocol profile, the packet is distributed to the VLAN ID of the protocol profile configured on the port.
- If the packet does not match the protocol profile, the packet is distributed to the default VLAN ID of the port.



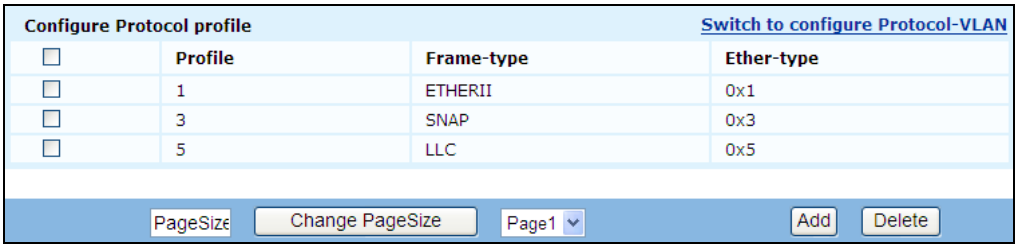
Add Protocol VLAN

Click Add to enter the interface for adding new protocol VLAN.

When configuring the protocol VLAN, multiple ports can be selected at the same time. **Profile** is the existing protocol profile number. If there is no protocol profile, configure the protocol profile first.

Configure Protocol Profile

Click Switch to configure protocol profile on the Configure Protocol-VLAN interface and you can configure the protocol profile.



Add Protocol Profile

Click Add to enter into the interface for adding new protocol profile.

Ether-type: The value range is 0x0001-0xffff.

Return to Interface for Configuring Protocol VLAN

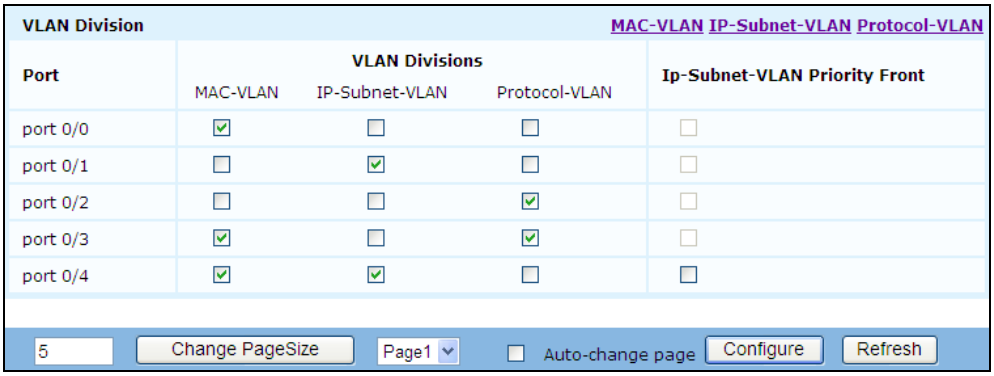
Click Switch to configure Protocol-VLAN on the Configure Protocol Profile interface and you can return to the interface for configuring the protocol VLAN.

VLAN Function Division

Overview

This section describes the VLAN function division configuration of the port.

By default, the order of the priorities of the four VLANs from high to low is MAC-based VLAN, IP subnet-based VLAN, protocol-based VLAN, and port-based VLAN. On one port, the divided VLAN takes effect by the priority and only one divided VLAN can take effect.



Ticking the check box means that the VLAN function is enabled on the port. Otherwise, disable the VLAN function.

Q-in-Q (Vlan dot1q tunnel) Configuration

This section describes the Vlan dot1q tunnel configuration.

Introduction to Vlan dot1q tunnel

Vlan dot1q tunnel is the expansion based on the 802.1Q protocol, that is, add another layer of 802.1Q tag (VLAN tag) to the original 802.1Q packet header. The two layers of tags make the number of VLANs become 4K×4K. QinQ encapsulates the VLAN Tag of the user's private network in the VLAN Tag of the public network so that the packet carries two layers of VLAN TAG to cross the backbone network (public network) of operators. In the public network, the packet is transmitted only according to the outer VLAN TAG (that is, VLAN TAG of the public network) and the VLAN TAG of the user's private network is screened, saving the VLAN IDs of the public network and providing a simple L2 VPN tunnel for users.

Vlan dot1q tunnel mapping is also the expansion based on 802.1Q. Different from Vlan dot1q tunnel, Vlan dot1q tunnel mapping is not to add one layer of 802.1Q tag to the original 802.1Q packet header, but replace the original 802.1Q tag with new 802.1Q tag. Therefore, the packet still carries only one layer of 802.1Q tag.

Basic Vlan dot1q tunnel Function

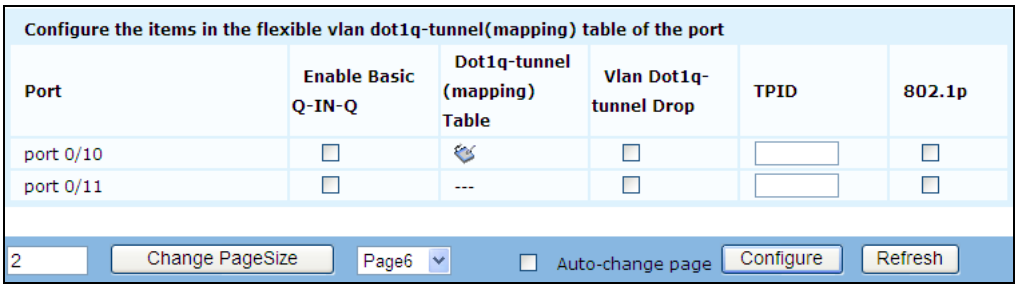
The Vlan dot1q tunnel function is enabled on the port. When the port receives one packet, it adds one layer of VLAN TAG to the packet. The

VLAN ID of the added Tag is the default VLAN ID of the port. If the received packet is the tag packet, it becomes the packet with two layers of Tag; if the received packet does not carry Tag, the packet becomes single-layer Tag packet.

Selective Vlan dot1q tunnel Function

The selective Vlan dot1q tunnel function cooperates with the port VLAN. The ports add specified outer VLAN Tag to the packet according to the selective Vlan dot1q tunnel (mapping) item and the VLAN ID in the packet tag. Vlan dot1q tunnel mapping is to replace the VLAN ID in the packet Tag with the specified VLAN ID. If the port does not match the selective Vlan dot1q tunnel (mapping) item, encapsulate the outer VLAN Tag for the packet. The VLAN Tag is the port PVID VLAN.

Q-IN-Q Configuration



TPID (Tag Protocol Identifier): It is one tag field in the packet and indicates the protocol type of the VLAN Tag. The value of the VLAN Tag field is 0x8100. The default value of the outer VLAN Tag in the Vlan dot1q tunnel packet is 0x8100. Different manufacturers may set different outer VLAN Tags for the Vlan dot1q tunnel packet, such as 0x9100.

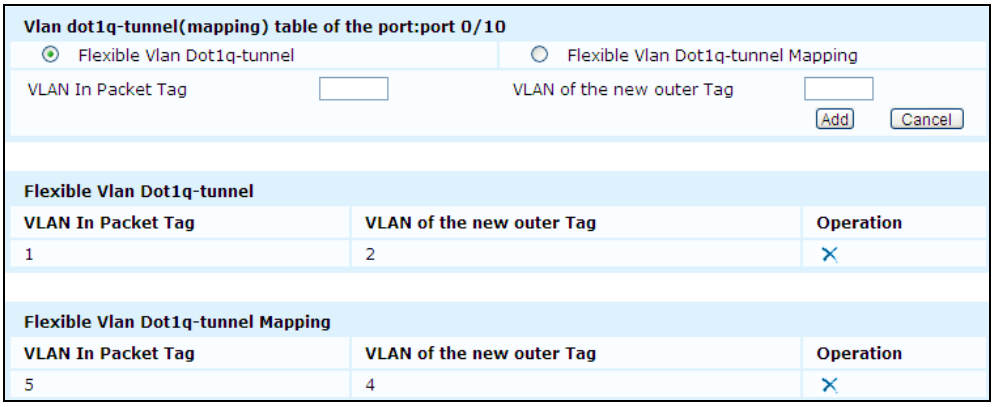
802.1p: Configure the value of the priority filed in the inner Tag of the port to be copied to the priority field in the outer Tag.

📖 Note

It means not to configure TPID.

Mapping Configuration

Click the icon for configuring the mapping to configure Q-IN-Q mapping on the port.



Note

When configuring new selective Vlan dot1q tunnel and if there are conflict items, the system automatically delete all conflict Vlan dot1q tunnel (mapping) items and then set new items.

L2 Protocol Control Configuration

This section describes the L2 protocol tunnel configuration.

Introduction to L2 protocol control

The L2 protocol control function is to control the L2 protocol packets received by the port. The L2 protocol control function can help to realize the following functions:

1. L2 protocol tunnel

It helps to transmit the L2 protocol packets such as BPDU and LACPDU of the customers' network transparently in the operators' network and realize the spanning tree calculation and link aggregation functions of the whole user network.

Enable the L2 protocol tunnel function on the port and the destination MAC address of the L2 protocol packet entering the port is replaced as the special multicast MAC address (by default, it is 01-00-0c-cd-cd-d0). The protocol packet is converted to the tunnel packet, which serves as the common L2 packet to be transmitted in the PVID VLAN of the port. When the tunnel packet is forwarded out from the port on which the L2 protocol tunnel function is enabled, the destination of the packet is recovered to the destination MAC address of the L2 protocol packet; the tunnel packet is replaced to common L2 packet to be sent out. The process of forwarding the tunnel packet out from the port on which the L2 protocol tunnel is not

enabled is the same as forwarding common L2 packet, complying with the forwarding principle in one VLAN. Enable the L2 protocol packet tunnel function on the two edge ports of the protocol tunnel to realize the tunnel function of the L2 protocol.

2. L2 protocol discard

It is to discard the L2 protocol packets such as BPDU and LACPDU received by the port directly so that the packets do not take part in the protocol processing.

3. L2 protocol peer

It is not to process the L2 protocol packets such as BPDU and LACPDU received by the port, but forward them to the upper protocol module to process. It is the default function.

Configure Special Multicast MAC for Replacing Destination MAC of L2 Protocol Packet

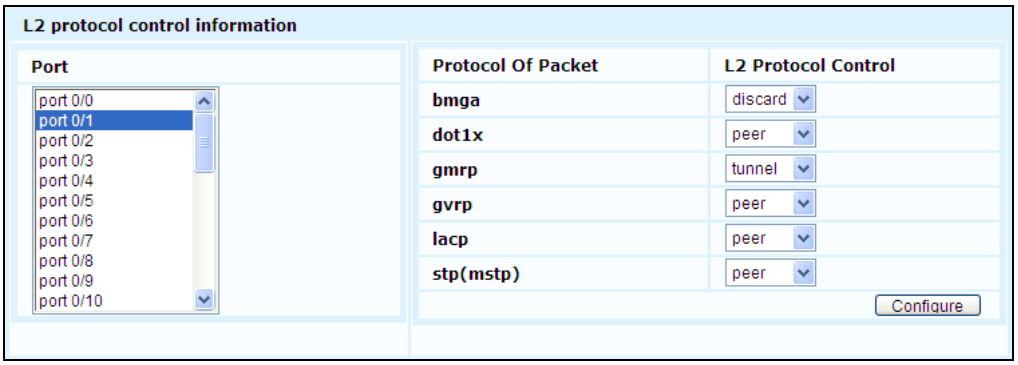
Note

The MAC address should be the one prompted in the command line and cannot be any other MAC address.

Caution

On the devices at the two sides of the L2 protocol tunnel, the configured special multicast MAC addresses for replacing the destination MAC addresses of the L2 protocol packets should be consistent.

L2 Protocol Control Configuration



Select the port from the left port list (multiple ports can be selected at the same time) and then configure the L2 protocol control.

Caution

When the port on which the L2 protocol tunnel function is enabled receives the corresponding L2 protocol tunnel packets, the system shuts down the port temporarily.

ACL Configuration

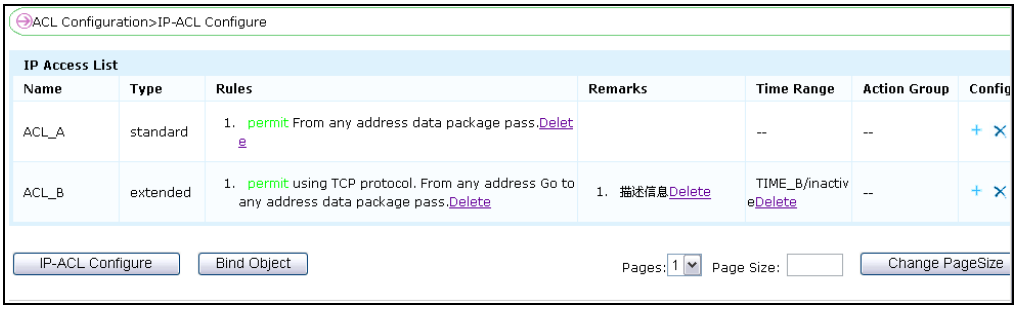
The full name of ACL is Access Control List, which is called Access List for short. The configurations related with the ACL function in Maipu S34xx switch include Action Group configuration, Traffic Meter configuration, and Time Range configuration.

Main contents:

- Configure IP standard access list
- Configure IP extended access list
- Configure MAC standard access list
- Configure MAC extended access list
- Configure Time Range
- Configure Action Group
- Configure Traffic Meter
- Apply ACL to Object

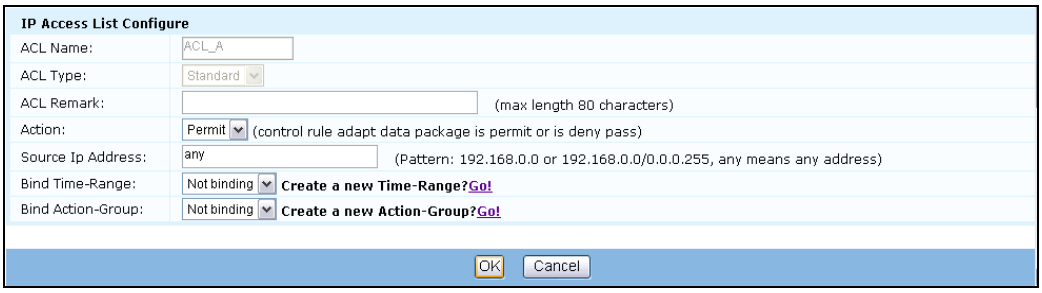
Configure IP Standard Access List

On the interface, you can view and configure the IP access control list (IP-ACL). The IP-ACL comprises one or more filtering rules. It permits or deny the packets by matching the information in the packet and the parameters in the access list. The filtering of the access list is a process from up to down. That is, if one packet matches one rule, execute the operation (permit or deny) of the rule. Otherwise, the packet is processed by matching the next filtering rule. If the packet does not match any rule, it is processed according to the default rule.



Add Rule

Click + to add one rule.



The operation brings in the name and type of the specified ACL, which cannot be changed.

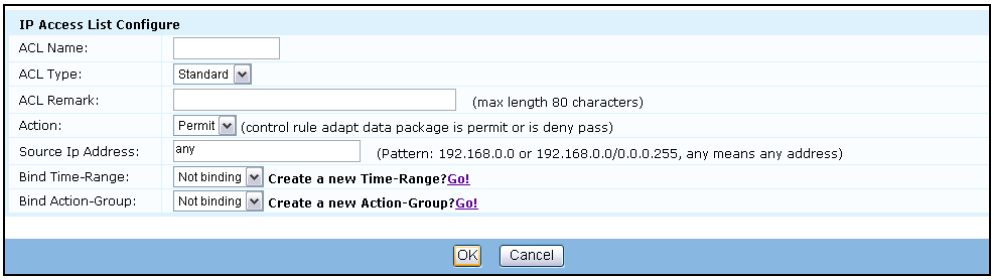
Delete

Click ✕ and you can delete one access list (if the access list is referenced, all configurations about the access list become invalid after the access list is deleted, but you can create an access list with the same name to recover).

Click Delete after one rule in the list and you can delete the rule (if the access list is bound to the interface, the system automatically deletes all bindings of the list on the interface after the list is deleted).

Create One IP Standard Access List

Click IP-ACL Configure to create one ACL.



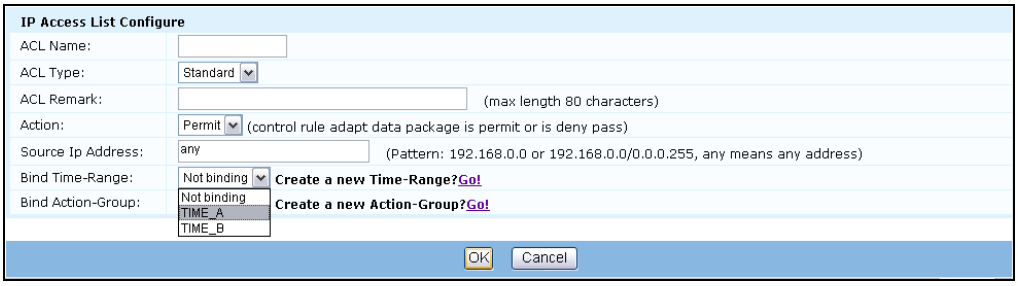
Create one IP standard access list, which can be named by numbers or by the user.

If using numbers to name the list, the four kinds of access lists have fixed number ranges.

Access List Type	Number Range
IP standard access list	1-1000
IP extended access list	1001-2000
MAC standard access list	2001-3000
MAC extended access list	3001-4000

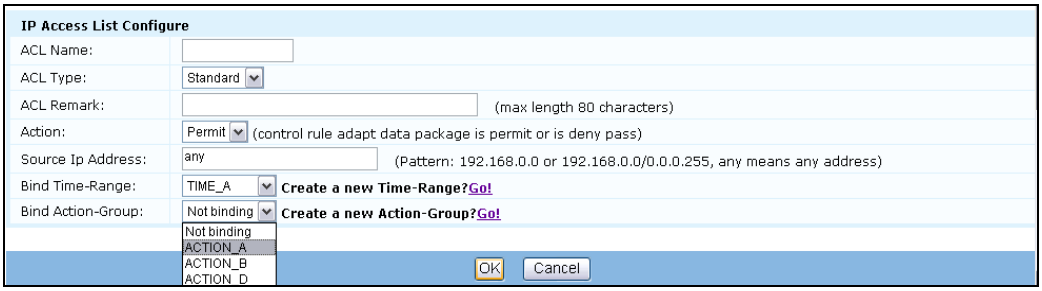
Bind Time Range

Select the existing time range to bind. You can also click **Create a new Time-Range** and then bind it.



Bind Action Group

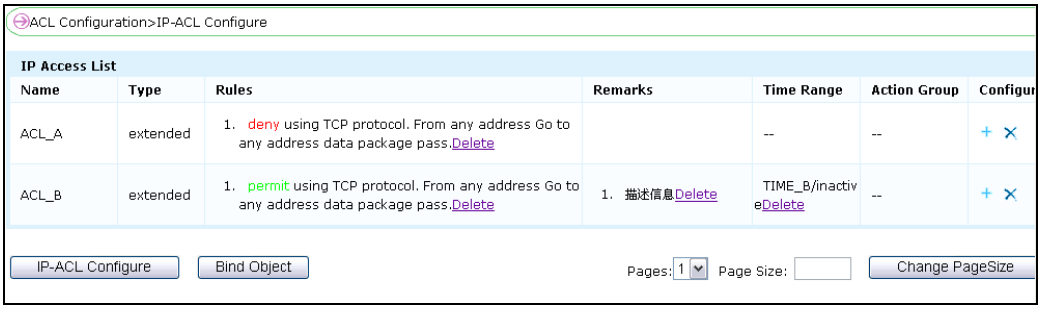
Select the existing action group to bind. You can also click **Create a new Action-Group** and then bind it.



For the operations of creating action group and time range, refer to time range configuration or action group configuration.

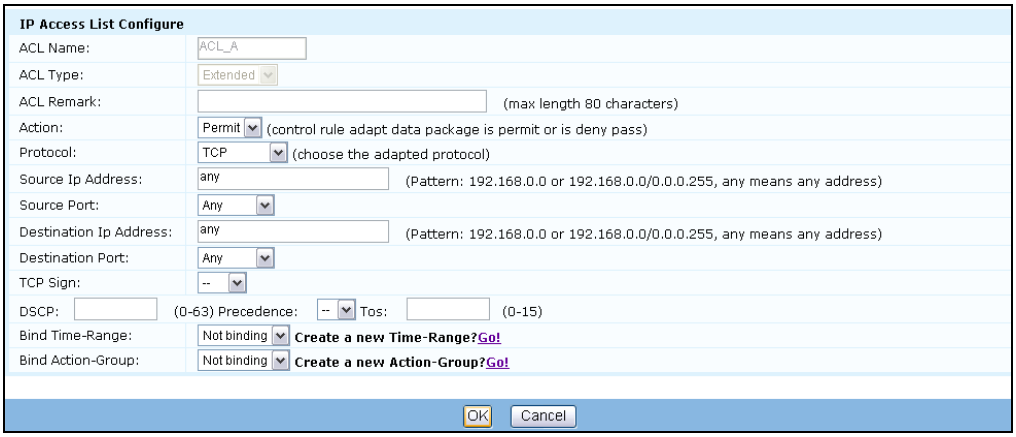
Configure IP Extended Access List

IP extended control list is to make the classification rules according to IP protocol number, source IP address, destination IP address, source TCP/UDP, destination TCP/UDP port number, packet priority, TCP tag, and IP fragment tag, and process the packet. The contents defined by IP extended access list are richer, more exact and more flexible than the IP standard access list.



Create One Rule

Click + to create one rule.



The operation brings in the name and type of the specified ACL, which cannot be changed.

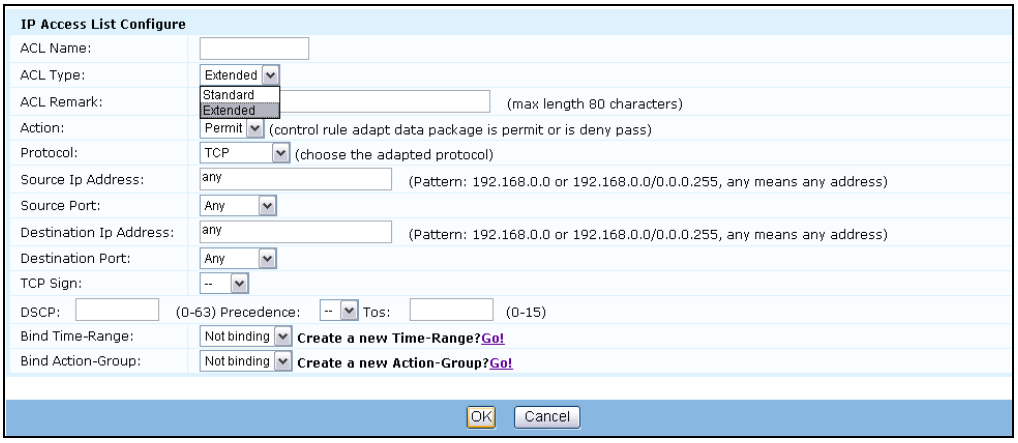
Delete

Click × and you can delete one access list (if the access list is referenced, all configurations about the access list become invalid after the access list is deleted, but you can create an access list with the same name to recover).

Click Delete after one rule in the list and you can delete the rule (if the access list is bound to the interface, the system automatically deletes all bindings of the list on the interface after the list is deleted).

Create One IP Extended Access List

Click IP-ACL Configure to create one ACL and select the type.

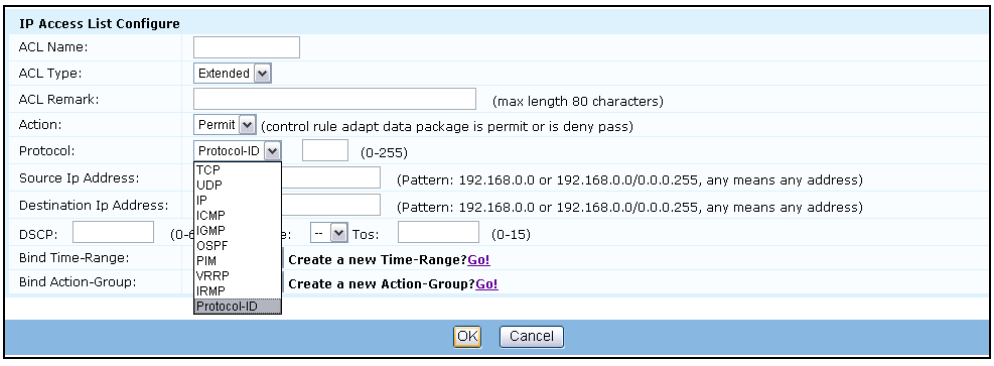


The ACL can be named by numbers or by the user. For naming by number, refer to the following table.

Access List Type	Number Range
IP standard access list	1-1000
IP extended access list	1001-2000
MAC standard access list	2001-3000
MAC extended access list	3001-4000

Protocol

Select the protocol to be matched. The system provides common protocols to select and you can also select the protocol number to specify the protocol.



DSCP

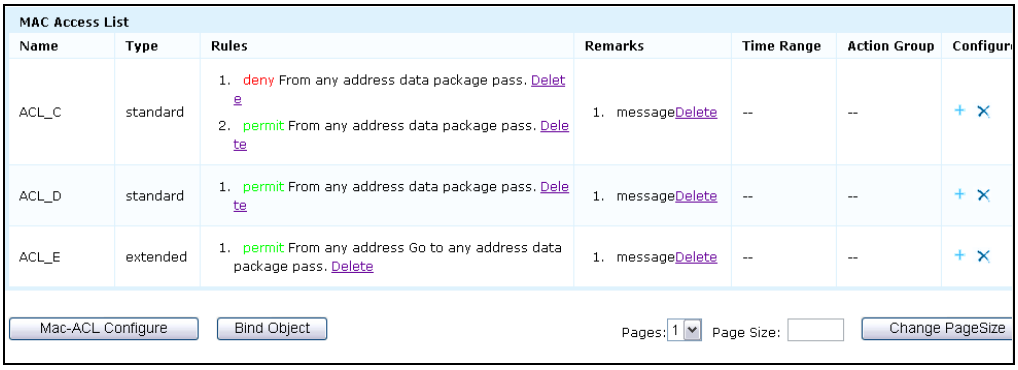
It is the differentiated services code point.

Bind Object

Click Bind Object to enter into the interface for binding object. For details, refer to the section of *Apply ACL to Object*.

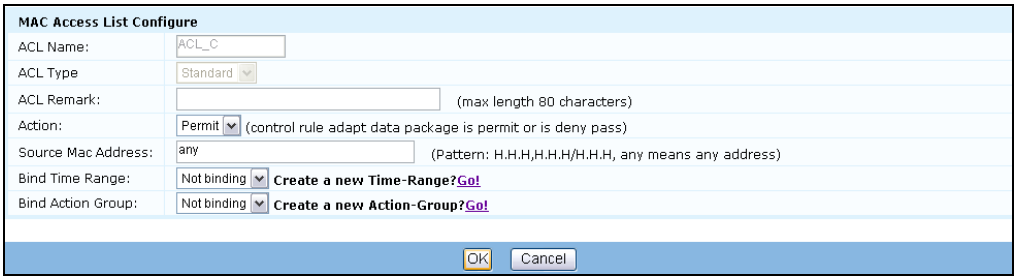
Configure MAC Standard Access List

MAC standard access list is to make rules only according to the source MAC address of the Ethernet packet and process the packet.



Create One Rule

Click + to create one rule.



The operation brings in the name and type of the specified ACL, which cannot be changed.

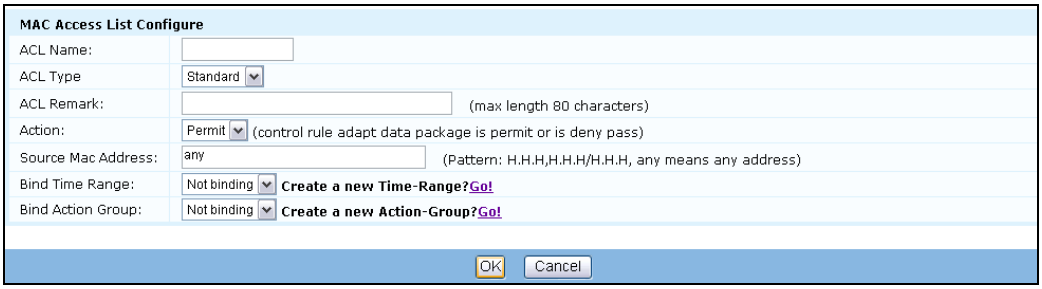
Delete

Click ✕ and you can delete one access list (if the access list is referenced, all configurations about the access list become invalid after the access list is deleted, but you can create an access list with the same name to recover).

Click Delete after one rule in the list and you can delete the rule (if the access list is bound to the interface, the system automatically deletes all bindings of the list on the interface after the list is deleted).

Create

Click Mac-ACL Configure to create one MAC-ACL.



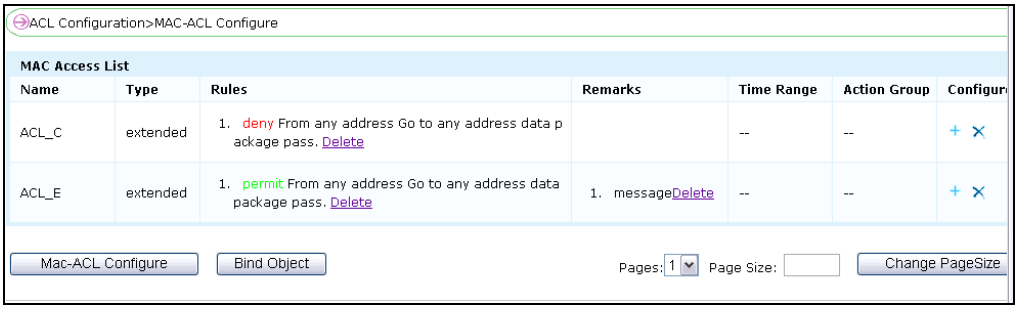
Create one MAC standard access list, which can be named by numbers or by the user. For naming by number, refer to the IP-ACL section.

Bind Object

For binding time range and action group, refer to the IP-ACL section.

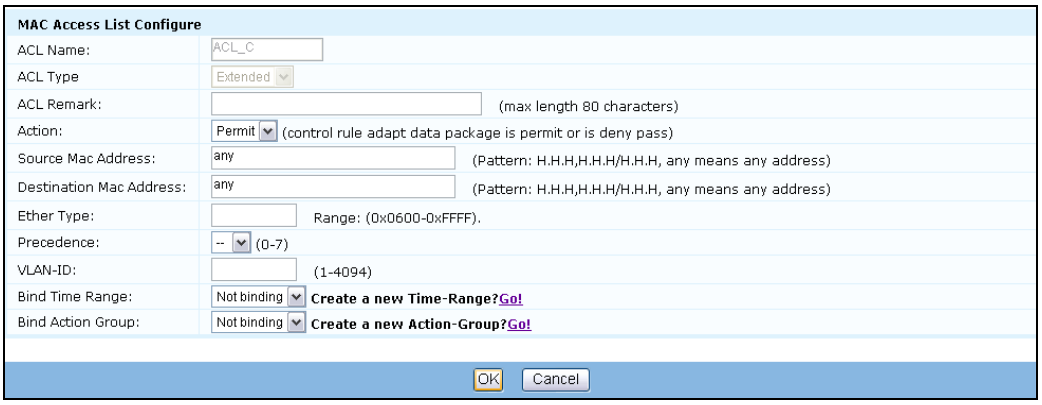
Configure MAC Extended Access List

MAC extended access list is to make rules according to source MAC address, destination MAC address, 802.1P priority, VLAN ID, and Ethernet type of the Ethernet packet, and process the packet.



Create One Rule

Click + to create one rule.



The operation brings in the name and type of the specified ACL, which cannot be changed.

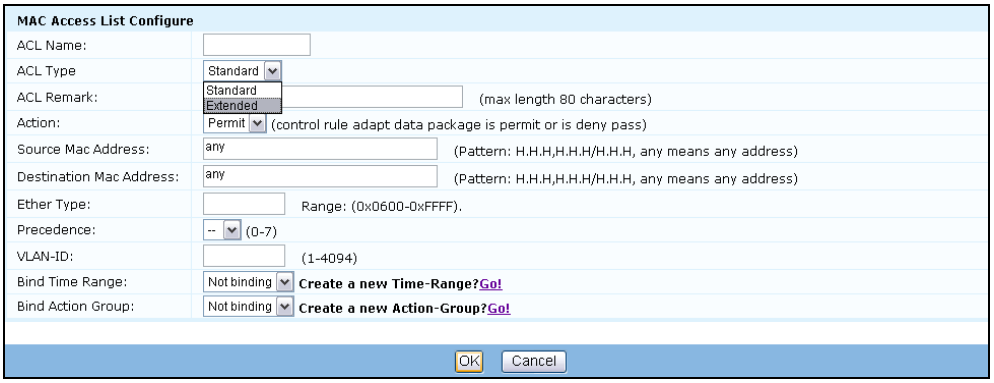
Delete

Click ✕ and you can delete one access list (if the access list is referenced, all configurations about the access list become invalid after the access list is deleted, but you can create an access list with the same name to recover).

Click Delete after one rule in the list and you can delete the rule (if the access list is bound to the interface, the system automatically deletes all bindings of the list on the interface after the list is deleted).

Create

Click Mac-ACL Configure to create one MAC extended access list and then select the type.



Create one MAC extended access list, which can be named by numbers or by the user. For naming by numbers, refer to the IP-ACL section.

Ethernet Type

The value range is 0x0600-0xFFFF.

The common types are:

- IP type: 0x0800
- ARP type: 0x0806

Precedence

The priority defined by IEEE802.1p and the value range is 0-7.

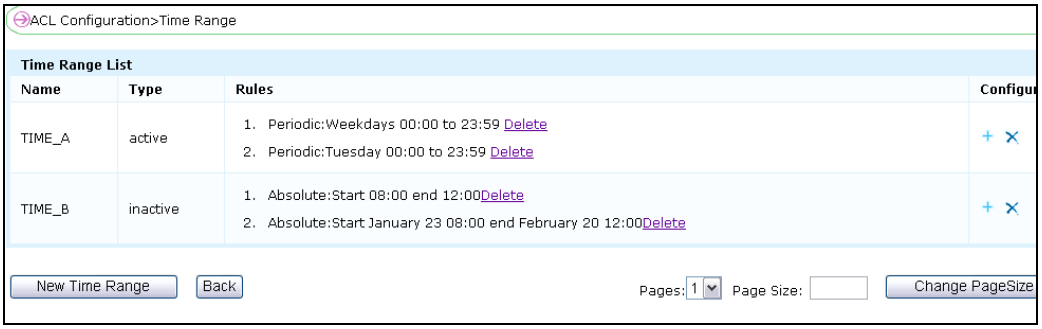
VLAN-ID

It is the VLAN number and the value range is 1-4094.

Configure Time Range

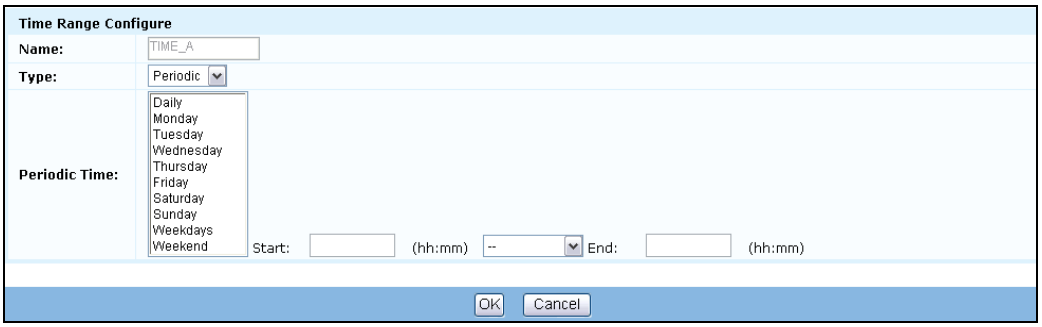
Time range is the time set. One time range includes 0-n time periods. The time range is the union set of the time periods. The **time-range** command is used to set the time range.

The status of the time range includes ACTIVE and INACTIVE. The status of the time range depends on the current status of the time periods in the time range. If any time period is in the ACTIVE state, the time range is in the ACTIVE state.



Create One Rule

Click + to create one time rule.



The operation brings in the name of the specified time range, which cannot be changed.

Delete

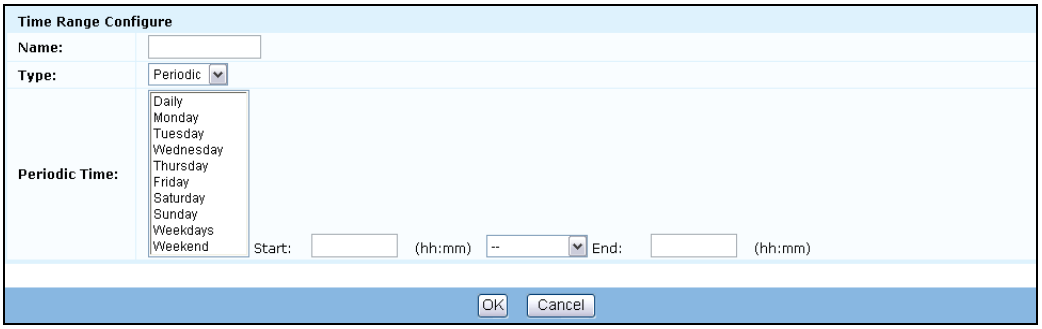
Click × and you can delete one time range (if the time range is referenced, all configurations about the time range become invalid after the time range is deleted, but you can create a time range with the same name to recover).

Click Delete after one time rule to delete the time rule.

Create

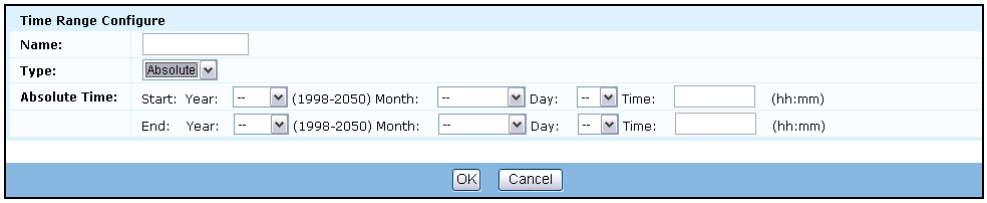
Click New Time Range to create one time range. The time range includes two kinds:

Periodic time range: It is required to configure one day or several days of each week, and the start time and the end time.



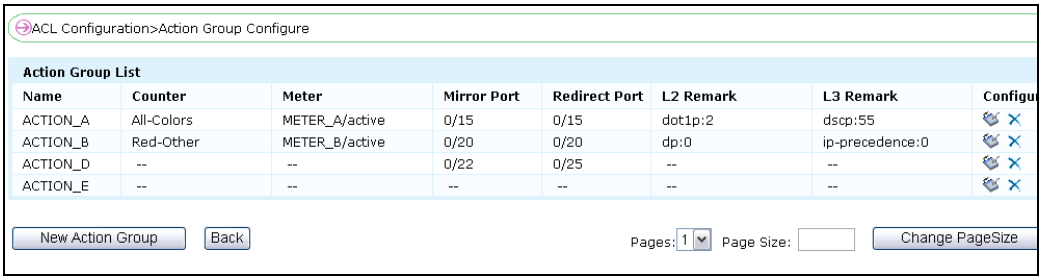
The name of the time range cannot begins with numbers and cannot exceed 31 characters.

Absolute time range: It is required to configure the year, month, day, hour and minute of the start time and end time.



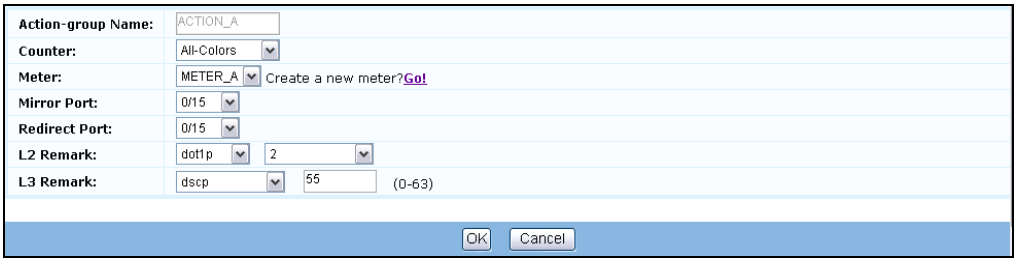
Configure Action Group

Action group is the action set. One action group can include packet mirroring, packet re-direction, packet modification, packet flow control, packet counting action.



Edit

Click to edit the attributes of the action group.



The operation brings in the action group name, which cannot be edited, but the other attributes can be edited.

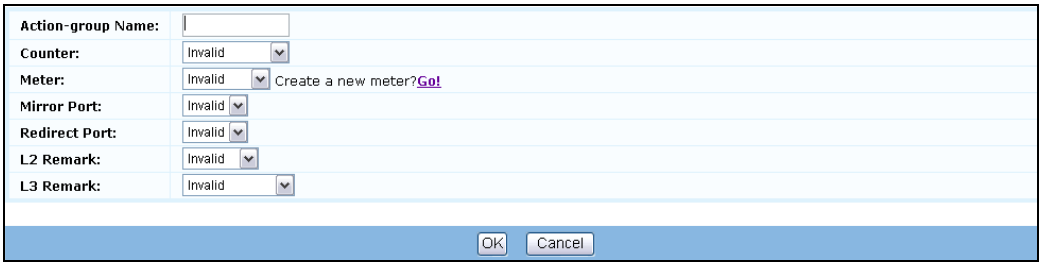
Delete

Click ✕ and you can delete one action group (if the action group is referenced, all configurations about the action group become invalid after the action group is deleted, but you can create an action group with the same name to recover).

Create

Click

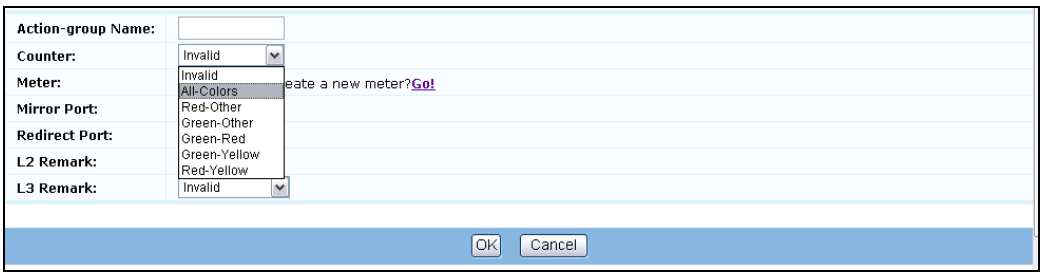
to create one action group.



The name of the action group cannot begin with numbers and comprises 31 characters at most.

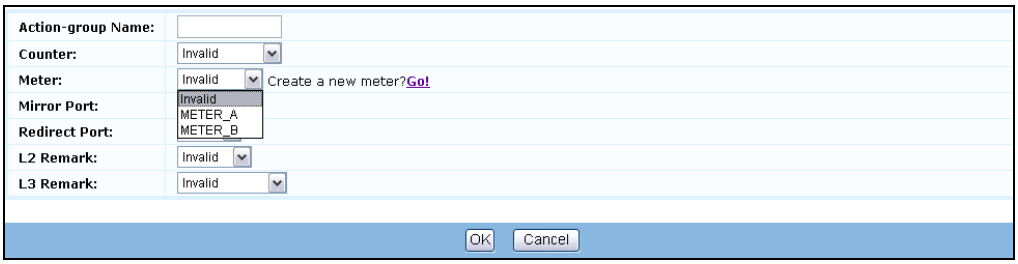
Counter

Configure the counting action in the action group. Configuring counting action is to count the matched packets.



Meter

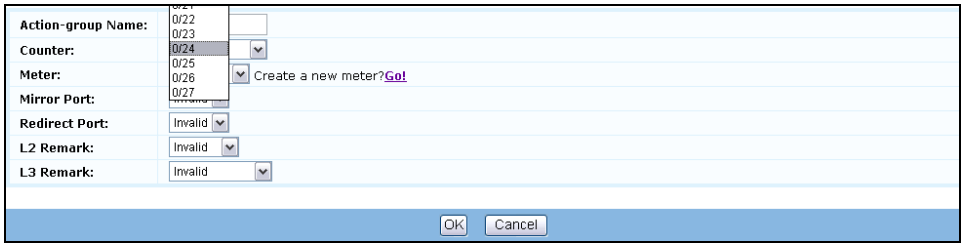
Configure the referenced meter name in the action group. Configuring meter is to limit or mark the matched packets.



Click **Create a new meter** to create a meter. For details, refer to *Configure Traffic Meter*.

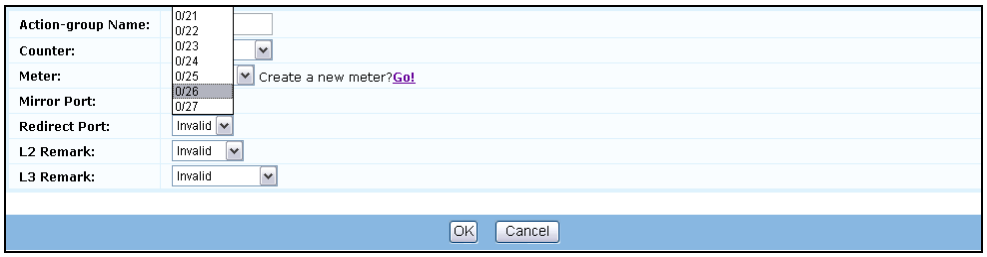
Mirror Port

Configure packet mirroring action in the action group. This is to mirror the matched packets to the specified port.



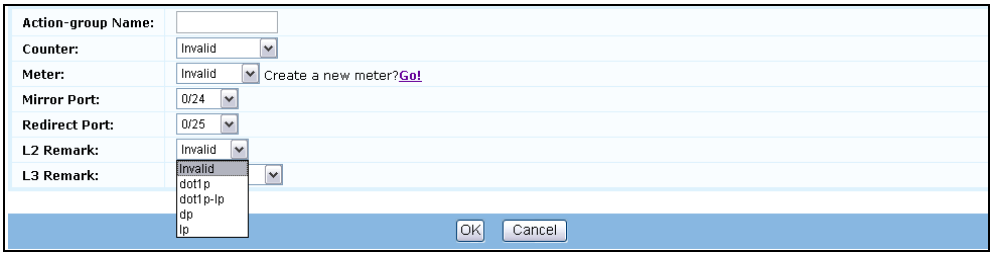
Re-direct Port

Configure packet re-directing action in the action group. The configuration is to re-direct the matched packet to the specified port.



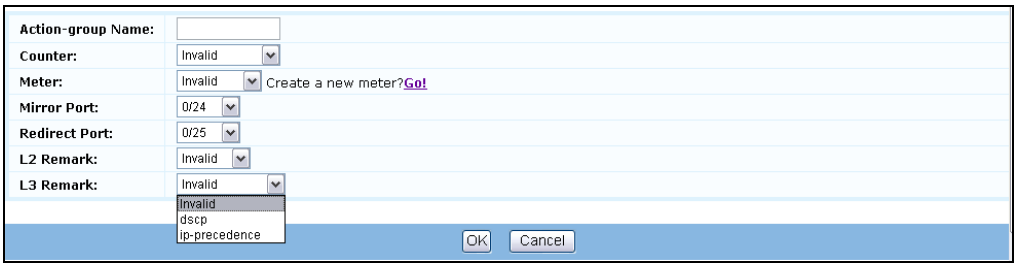
Configure L2 Remark

Configure the L2 packet remarking action in the action group. The configuration is to classify the matched packets so that the user can adopt different QoS policies in the later data communication.



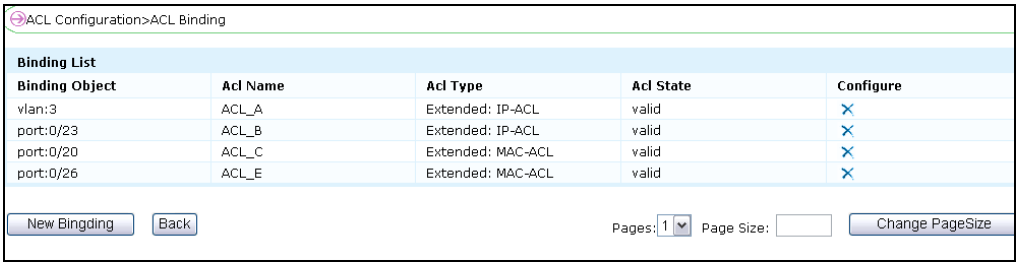
Configure L3 Remark

Configure the L3 packet remarking action in the action group. The configuration is to classify the matched packets so that the user can adopt different QoS policies in the later data communication.



Apply ACL to Object

After setting up one access list, it can be applied on one or more objects, so as to realize the function of filtering ACL packets. In Maipu S34xx switch, the access list can only be applied at the input direction of the object. The objects include port object, global object, and VLAN object.

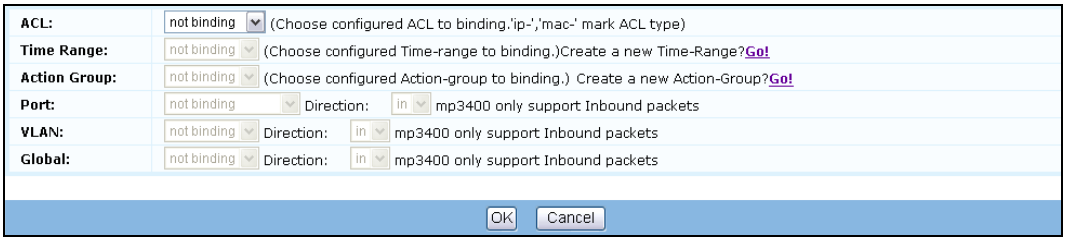


Delete

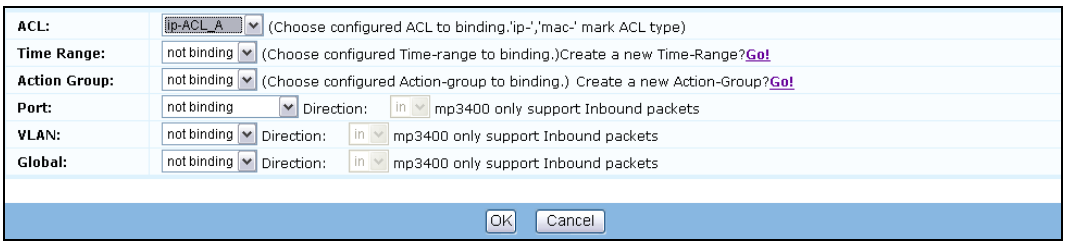
Click ✕ and you can delete the binding relation between the binding object and ACL (deleting the binding time domain and action group is performed on the corresponding ACL interface).

Apply

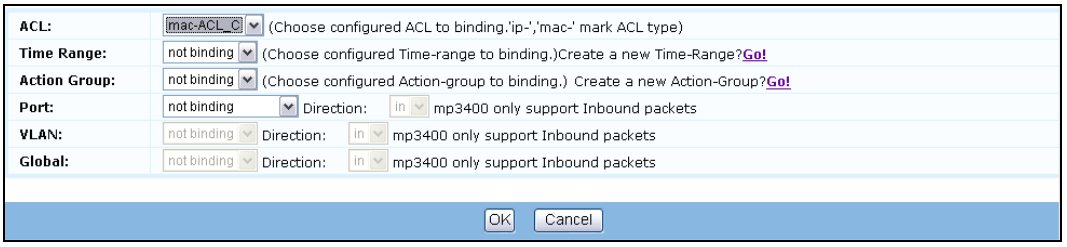
Click **New Binding** to apply ACL to object.



Ip-acl can be applied to all objects.



Mac-acl cannot be applied to VLAN or global.



📖 Note

Viewing and deleting the time range and action group bound to ACL are performed on the interface of the bound ACL.

S3400 switch only supports the ACL at the in direction, so the direction is grayed and unavailable.

QoS Configuration

This chapter describes the QoS usage and configuration of the port.

Main contents:

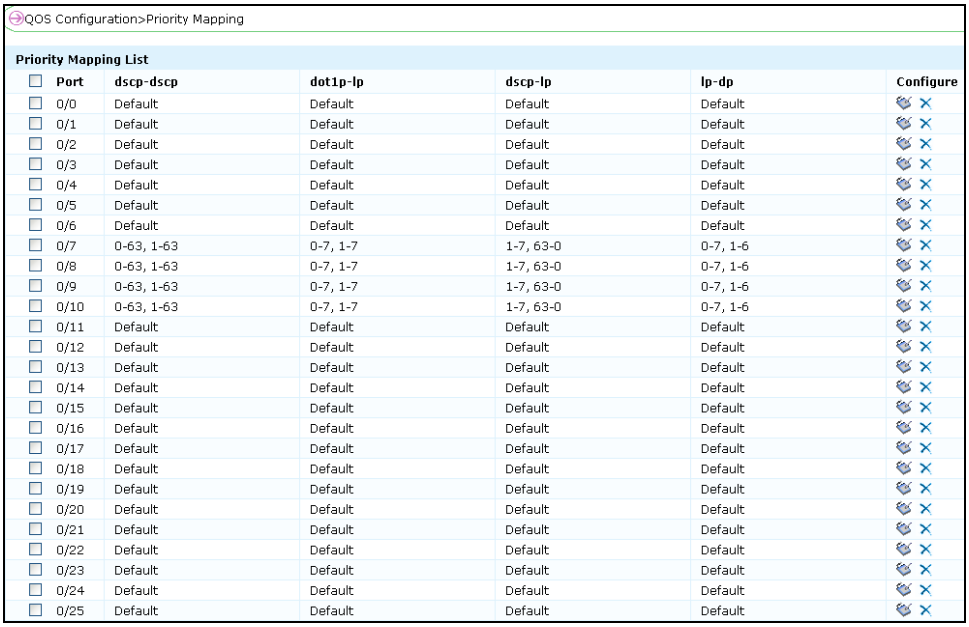
- Priority mapping
- Queue scheduling mode
- Dropping mode
- Speed limitation
- Port flow shaping
- Port queue flow shaping

Priority Mapping

The priority mapping is to map to the local priority according to the dscp or 802.1p value of the packet. And then the local priority maps to the corresponding drop priority. The priority mapping is to configure the relation of theses mappings.

The mapping relation is as follows:

1. dscp-lp mapping: Map to the local priority IP value according to the DSCP value of the packet;
2. dot1p-lp mapping: Map to the local priority IP according to the 802.1p priority of the packet;
3. lp-dp mapping: Map to the drop priority according to the local priority. The smaller the drop priority, the earlier the packet is dropped. The drop priority corresponds to the queue on the port. The packet with dp as o is input to queue 0; the packet with dp as 1 is input to queue 1…;
4. dscp-dscp mapping: Modify the dscp value of the packet according to the dscp of the packet;



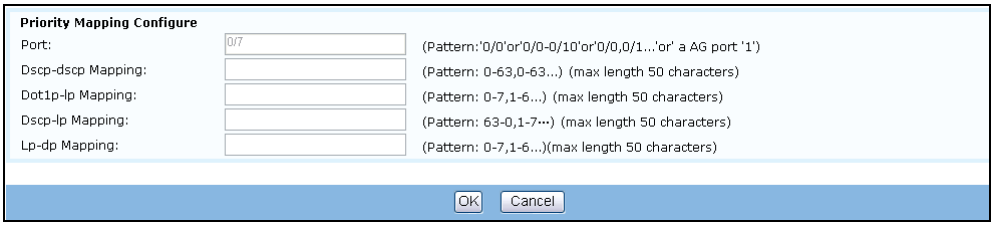
Port	dscp-dscp	dot1p-lp	dscp-lp	lp-dp	Configure
0/0	Default	Default	Default	Default	
0/1	Default	Default	Default	Default	
0/2	Default	Default	Default	Default	
0/3	Default	Default	Default	Default	
0/4	Default	Default	Default	Default	
0/5	Default	Default	Default	Default	
0/6	Default	Default	Default	Default	
0/7	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6	
0/8	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6	
0/9	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6	
0/10	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6	
0/11	Default	Default	Default	Default	
0/12	Default	Default	Default	Default	
0/13	Default	Default	Default	Default	
0/14	Default	Default	Default	Default	
0/15	Default	Default	Default	Default	
0/16	Default	Default	Default	Default	
0/17	Default	Default	Default	Default	
0/18	Default	Default	Default	Default	
0/19	Default	Default	Default	Default	
0/20	Default	Default	Default	Default	
0/21	Default	Default	Default	Default	
0/22	Default	Default	Default	Default	
0/23	Default	Default	Default	Default	
0/24	Default	Default	Default	Default	
0/25	Default	Default	Default	Default	

If the mapping is not configured, it is displayed as default.

Edit

Edit Single Priority Mapping

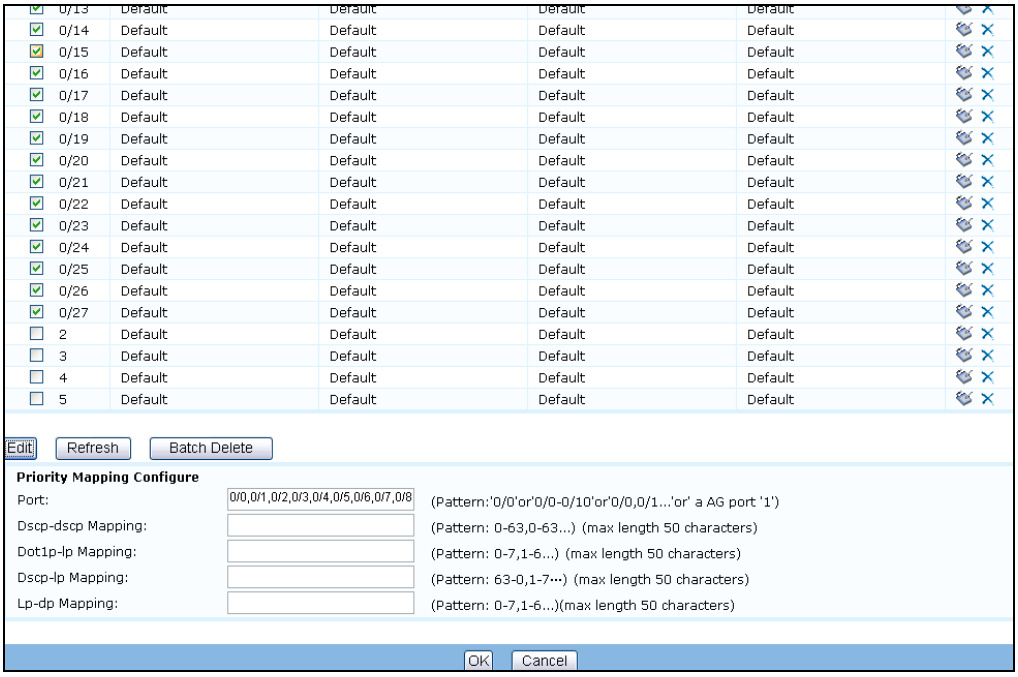
Click to edit the priority mapping of the port.



On the interface, there is the selected port, which cannot be modified. The mappings of the port can be modified.

Batch Edit

Click and you can edit the priorities of all selected ports.



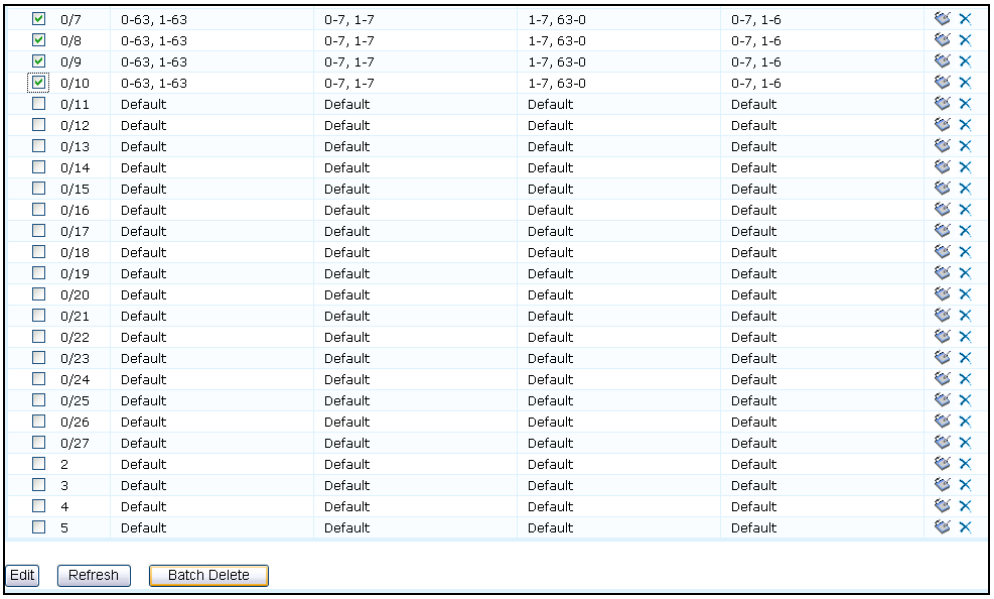
Delete

Delete Single Priority Mapping

Click to delete all priority mappings of the port.

Batch Delete

Click to delete all priority mappings of the selected port.



☑	0/7	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6
☑	0/8	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6
☑	0/9	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6
☑	0/10	0-63, 1-63	0-7, 1-7	1-7, 63-0	0-7, 1-6
☐	0/11	Default	Default	Default	Default
☐	0/12	Default	Default	Default	Default
☐	0/13	Default	Default	Default	Default
☐	0/14	Default	Default	Default	Default
☐	0/15	Default	Default	Default	Default
☐	0/16	Default	Default	Default	Default
☐	0/17	Default	Default	Default	Default
☐	0/18	Default	Default	Default	Default
☐	0/19	Default	Default	Default	Default
☐	0/20	Default	Default	Default	Default
☐	0/21	Default	Default	Default	Default
☐	0/22	Default	Default	Default	Default
☐	0/23	Default	Default	Default	Default
☐	0/24	Default	Default	Default	Default
☐	0/25	Default	Default	Default	Default
☐	0/26	Default	Default	Default	Default
☐	0/27	Default	Default	Default	Default
☐	2	Default	Default	Default	Default
☐	3	Default	Default	Default	Default
☐	4	Default	Default	Default	Default
☐	5	Default	Default	Default	Default

Edit Refresh Batch Delete

Queue Scheduling Mode

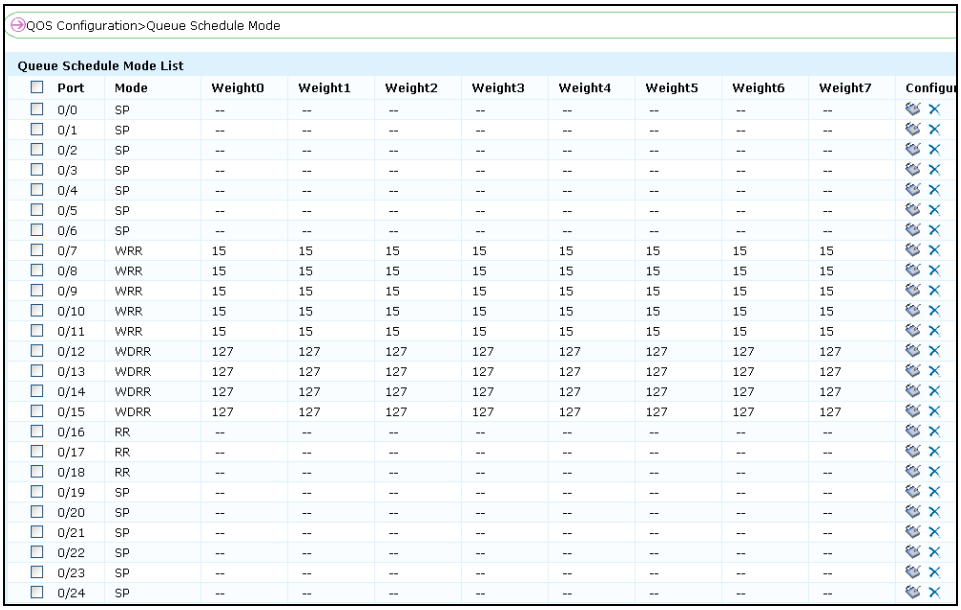
Each port has eight output queues. The following scheduling policies can be adopted:

SP (Strict Priority): Queue 7 has the highest priority and queue 0 has the lowest priority;

RR (Round Robin): Packet-based fair scheduling. As long as one queue schedules one packet, turn to the next queue;

WRR (Weighted Round Robin): Packet-based weighted scheduling. You can configure how many packets are scheduled by each queue before turning to the next queue. When it is configured as 0, it indicates strict priority queue;

WDRR (Weighted Deficit Round Robin): It is an improvement for the WRR algorithm.



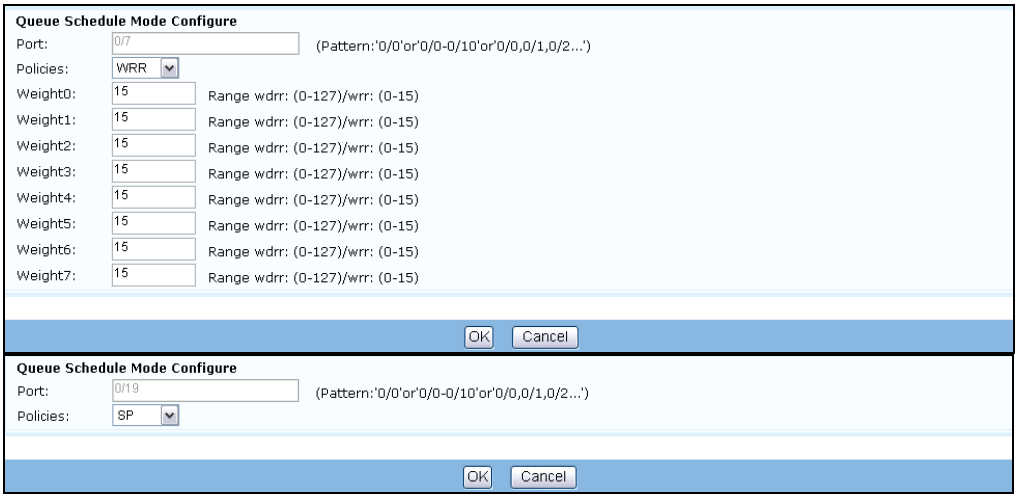
Port	Mode	Weight0	Weight1	Weight2	Weight3	Weight4	Weight5	Weight6	Weight7	Configu
0/0	SP	--	--	--	--	--	--	--	--	
0/1	SP	--	--	--	--	--	--	--	--	
0/2	SP	--	--	--	--	--	--	--	--	
0/3	SP	--	--	--	--	--	--	--	--	
0/4	SP	--	--	--	--	--	--	--	--	
0/5	SP	--	--	--	--	--	--	--	--	
0/6	SP	--	--	--	--	--	--	--	--	
0/7	WRR	15	15	15	15	15	15	15	15	
0/8	WRR	15	15	15	15	15	15	15	15	
0/9	WRR	15	15	15	15	15	15	15	15	
0/10	WRR	15	15	15	15	15	15	15	15	
0/11	WRR	15	15	15	15	15	15	15	15	
0/12	WDRR	127	127	127	127	127	127	127	127	
0/13	WDRR	127	127	127	127	127	127	127	127	
0/14	WDRR	127	127	127	127	127	127	127	127	
0/15	WDRR	127	127	127	127	127	127	127	127	
0/16	RR	--	--	--	--	--	--	--	--	
0/17	RR	--	--	--	--	--	--	--	--	
0/18	RR	--	--	--	--	--	--	--	--	
0/19	SP	--	--	--	--	--	--	--	--	
0/20	SP	--	--	--	--	--	--	--	--	
0/21	SP	--	--	--	--	--	--	--	--	
0/22	SP	--	--	--	--	--	--	--	--	
0/23	SP	--	--	--	--	--	--	--	--	
0/24	SP	--	--	--	--	--	--	--	--	

The SP and RR modes have no weight values, so they are displayed “--".

Edit

Edit Single Queue Scheduling

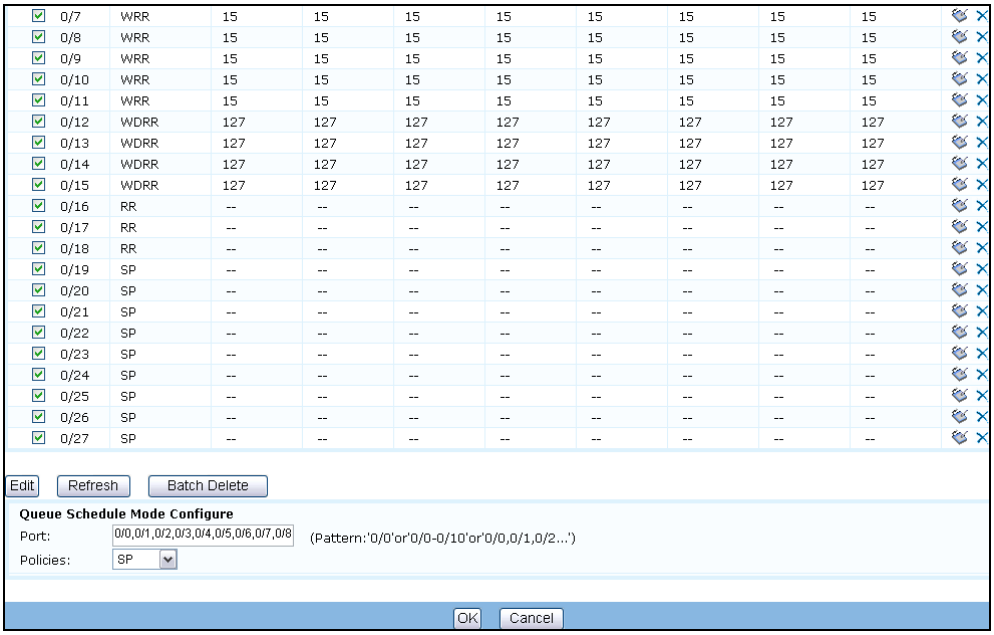
Click to edit the queue scheduling mode of the port.



On the interface, there is the selected port and policies. The policies can be modified.

Batch Edit

Click to edit the queue scheduling mode of the selected port.



The default value is the SP mode.

Delete

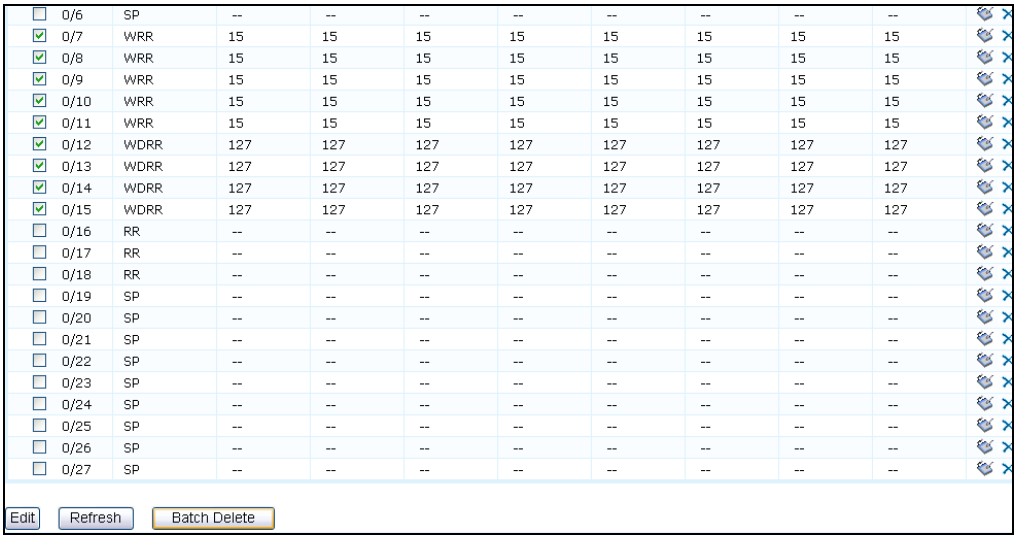
Delete Single Queue Scheduling

Click to delete the queue scheduling mode of the port and recover to the SP mode.

Batch Delete

Click

to delete the queue scheduling mode of the selected port and recover to the SP mode.

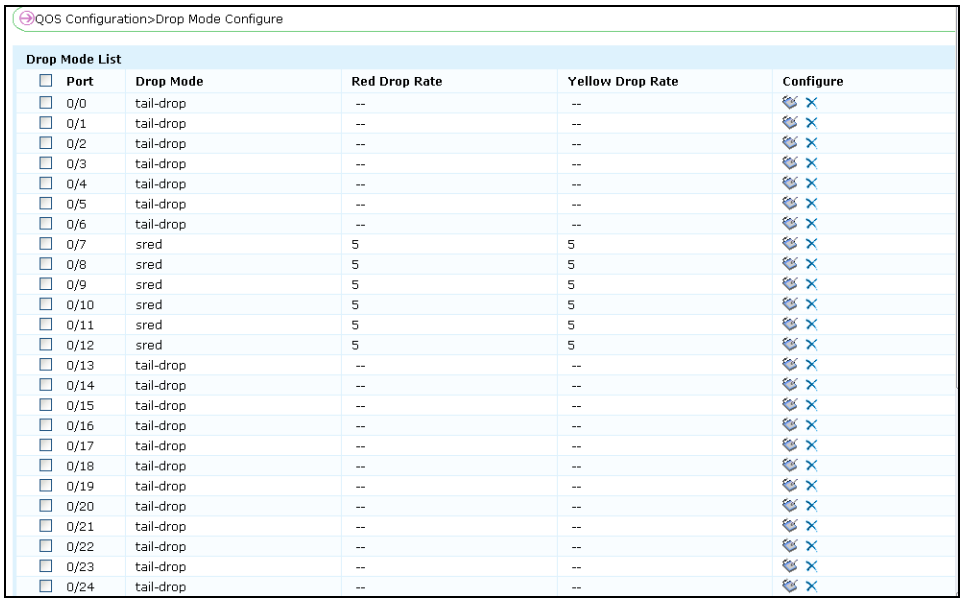


☐	0/6	SP	--	--	--	--	--	--	--	--
☑	0/7	WRR	15	15	15	15	15	15	15	15
☑	0/8	WRR	15	15	15	15	15	15	15	15
☑	0/9	WRR	15	15	15	15	15	15	15	15
☑	0/10	WRR	15	15	15	15	15	15	15	15
☑	0/11	WRR	15	15	15	15	15	15	15	15
☑	0/12	WDRR	127	127	127	127	127	127	127	127
☑	0/13	WDRR	127	127	127	127	127	127	127	127
☑	0/14	WDRR	127	127	127	127	127	127	127	127
☑	0/15	WDRR	127	127	127	127	127	127	127	127
☐	0/16	RR	--	--	--	--	--	--	--	--
☐	0/17	RR	--	--	--	--	--	--	--	--
☐	0/18	RR	--	--	--	--	--	--	--	--
☐	0/19	SP	--	--	--	--	--	--	--	--
☐	0/20	SP	--	--	--	--	--	--	--	--
☐	0/21	SP	--	--	--	--	--	--	--	--
☐	0/22	SP	--	--	--	--	--	--	--	--
☐	0/23	SP	--	--	--	--	--	--	--	--
☐	0/24	SP	--	--	--	--	--	--	--	--
☐	0/25	SP	--	--	--	--	--	--	--	--
☐	0/26	SP	--	--	--	--	--	--	--	--
☐	0/27	SP	--	--	--	--	--	--	--	--

Edit Refresh Batch Delete

Drop Mode

The port supports two drop modes, including Tail Drop and sRED. sRED is a simple random early drop algorithm, which begins to drop a color of packets before the queue is full. It has two queue thresholds, including low threshold and high threshold. Every time one packet to enter the queue is received, check the current queue depth. If the queue depth is lower than the low threshold, the packet enters the queue; if the queue depth is higher than the high threshold, the packet is dropped. If the queue depth is between the low threshold and the high threshold, whether the packet is dropped depends on the configured drop rate.



QOS Configuration>Drop Mode Configure

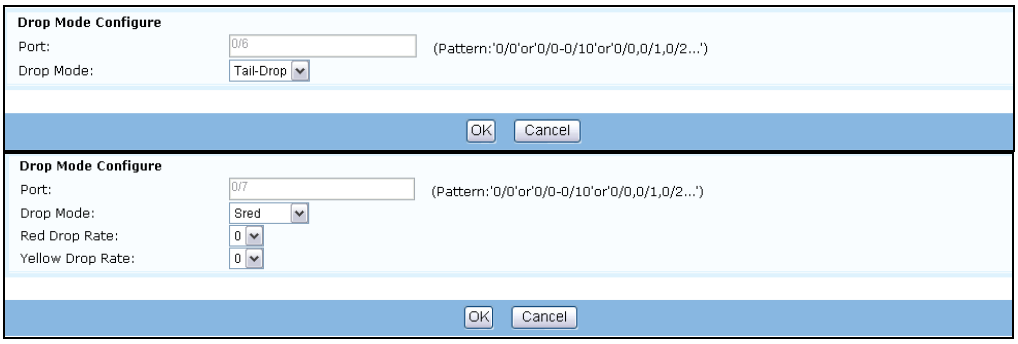
Drop Mode List

	Port	Drop Mode	Red Drop Rate	Yellow Drop Rate	Configure
☐	0/0	tail-drop	--	--	
☐	0/1	tail-drop	--	--	
☐	0/2	tail-drop	--	--	
☐	0/3	tail-drop	--	--	
☐	0/4	tail-drop	--	--	
☐	0/5	tail-drop	--	--	
☐	0/6	tail-drop	--	--	
☐	0/7	sred	5	5	
☐	0/8	sred	5	5	
☐	0/9	sred	5	5	
☐	0/10	sred	5	5	
☐	0/11	sred	5	5	
☐	0/12	sred	5	5	
☐	0/13	tail-drop	--	--	
☐	0/14	tail-drop	--	--	
☐	0/15	tail-drop	--	--	
☐	0/16	tail-drop	--	--	
☐	0/17	tail-drop	--	--	
☐	0/18	tail-drop	--	--	
☐	0/19	tail-drop	--	--	
☐	0/20	tail-drop	--	--	
☐	0/21	tail-drop	--	--	
☐	0/22	tail-drop	--	--	
☐	0/23	tail-drop	--	--	
☐	0/24	tail-drop	--	--	

Edit

Edit Single

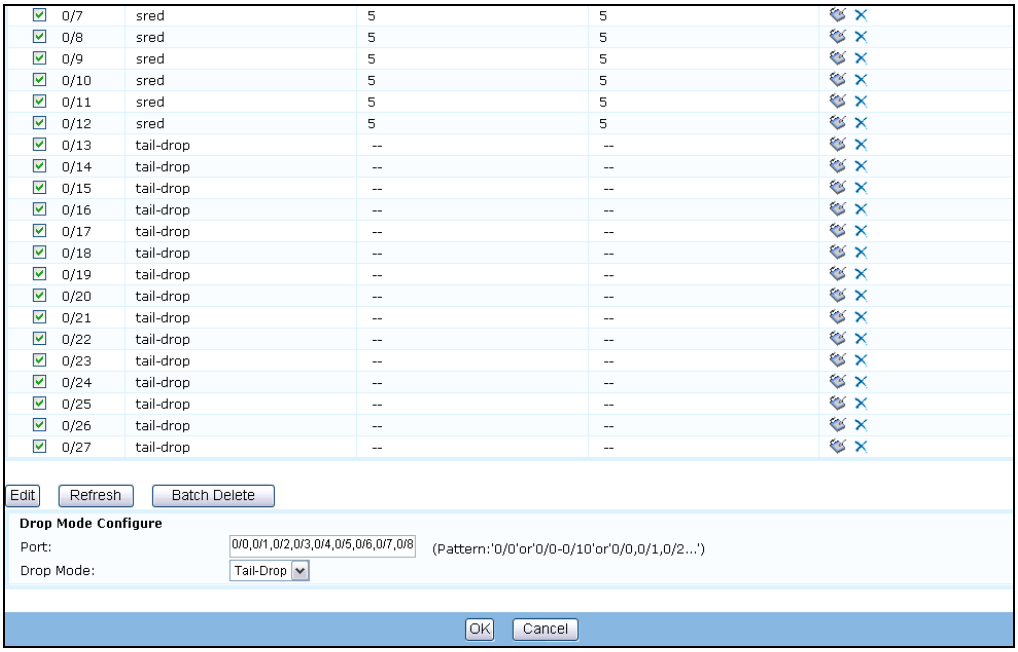
Click to edit the corresponding drop mode.



On the interface, there is the selected port and the drop mode. The port cannot be modified.

Batch Edit

Click Edit to edit the drop mode of the selected port.



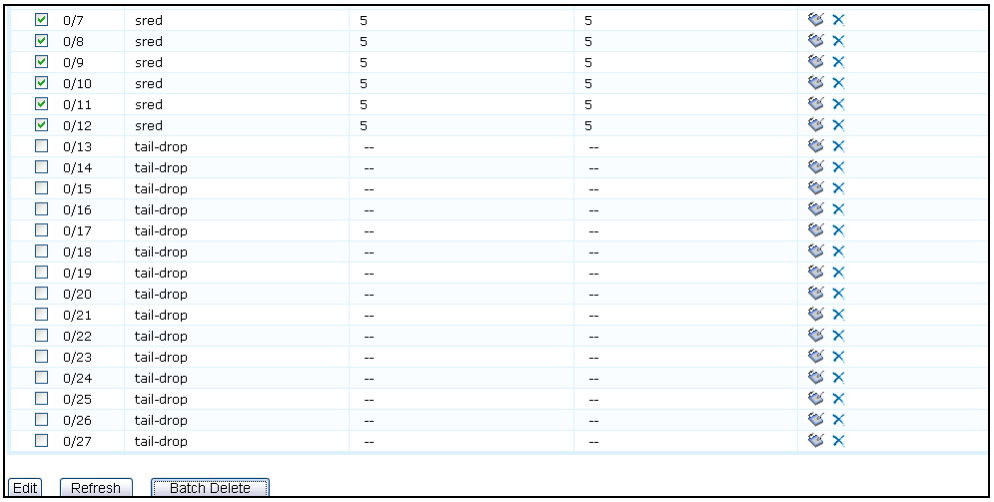
Delete

Delete Single

Click ✕ to delete the drop mode of the port. The default value is tail-drop.

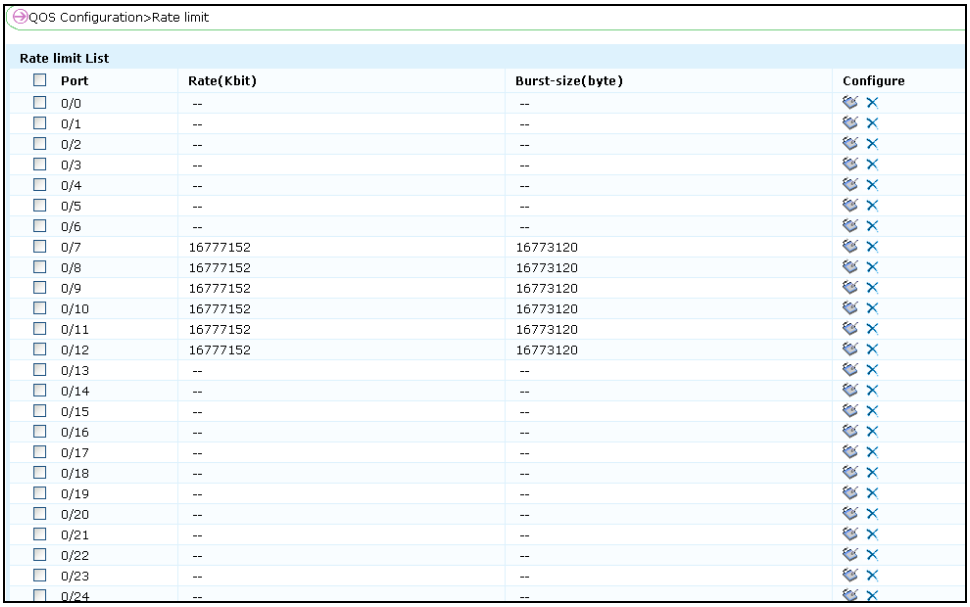
Batch Delete

Click Batch Delete to delete the drop modes of the selected ports. The default value is tail-drop.



Rate Limitation

To ensure that that the information flow over the network does not overload and cause blocking. Maipu series switches provide port-based speed limitation at the input direction, that is, limit the total speed at the receiving direction of the port and the overloading flow is dropped. The configured parameters are bandwidth threshold (Kbit, 64K is the minimum granularity and the burst flow (bytes).

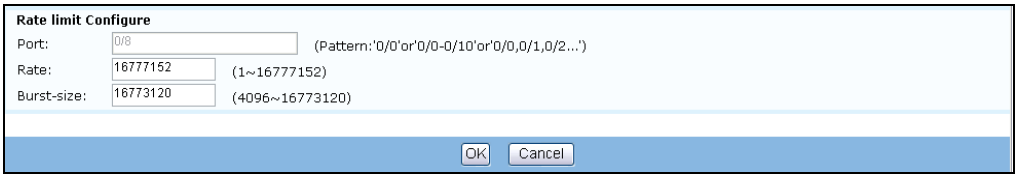


The un-configured speed limitation is displayed as --.

Edit

Edit Single

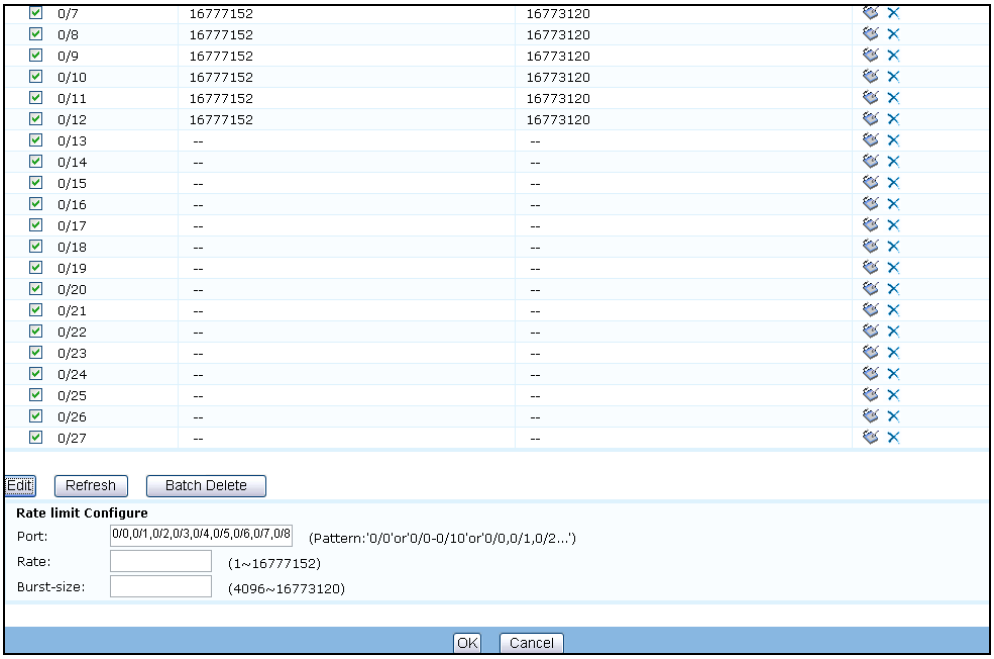
Click to edit the corresponding port speed limitation.



On the interface, there is the selected port and the related parameter values for modification. The port cannot be modified.

Batch Edit

Click to edit the speed limitation of the selected ports.



On the interface, there are the selected ports. You can also input the desired ports according to the port format.

Delete

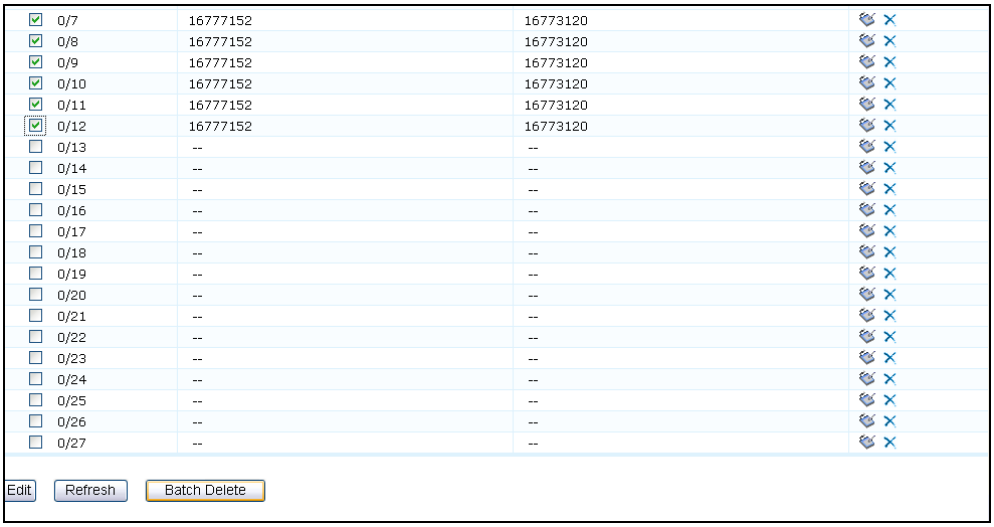
Delete Single

Click to delete the speed limitation of the corresponding port and recover to the default value --.

Batch Delete

Click

to delete the speed limitations of all selected ports and recover to the default value --.



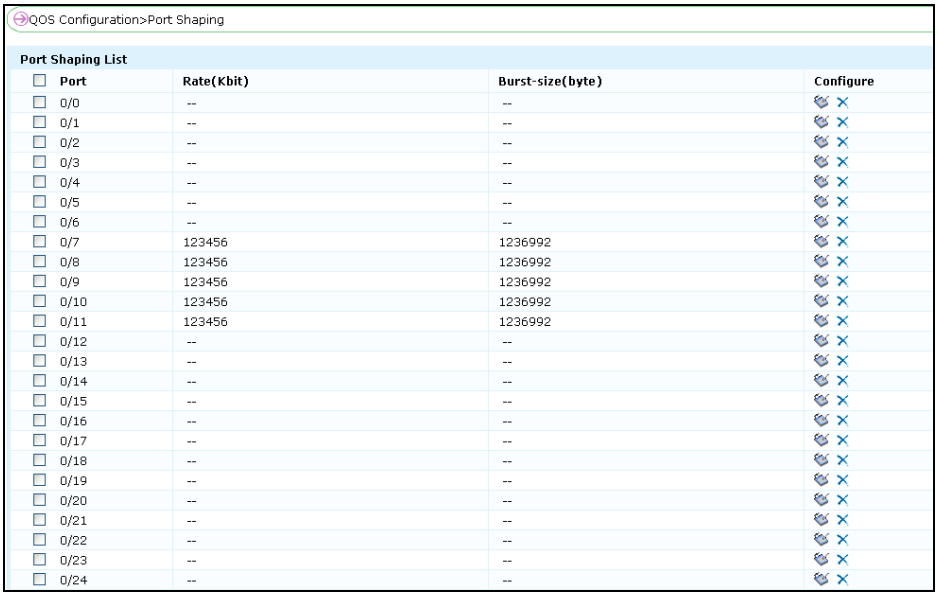
0/7	16777152	16773120	
0/8	16777152	16773120	
0/9	16777152	16773120	
0/10	16777152	16773120	
0/11	16777152	16773120	
0/12	16777152	16773120	
0/13	--	--	
0/14	--	--	
0/15	--	--	
0/16	--	--	
0/17	--	--	
0/18	--	--	
0/19	--	--	
0/20	--	--	
0/21	--	--	
0/22	--	--	
0/23	--	--	
0/24	--	--	
0/25	--	--	
0/26	--	--	
0/27	--	--	

Edit Refresh Batch Delete

Port Flow Shaping

Port-based flow shaping at the output direction makes packets be sent out with even speed. The configured parameters are bandwidth threshold (Kbit, 64K is the minimum granularity and the burst flow (bytes). The burst flow step length is 4K bytes.

Configure the flow shaping. The input parameters may be inconsistent with the actual configured values, because the driver adjusts the input value according to the chip. The last value of rate is an integer multiple of 64. When the input value is not the integer multiple of 64, the driver adjusts it to the minimum integer multiple of 64, which is larger than the current value. The value of burst-size after modification is an integer multiple of 4096.



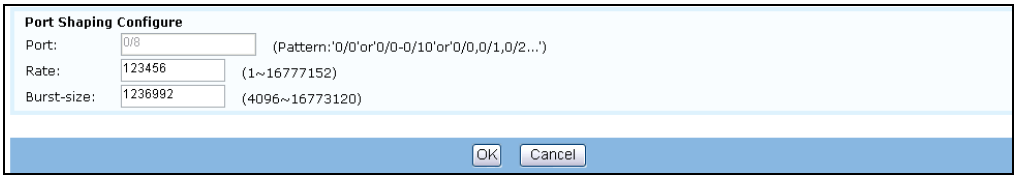
Port	Rate(Kbit)	Burst-size(byte)	Configure
0/0	--	--	
0/1	--	--	
0/2	--	--	
0/3	--	--	
0/4	--	--	
0/5	--	--	
0/6	--	--	
0/7	123456	1236992	
0/8	123456	1236992	
0/9	123456	1236992	
0/10	123456	1236992	
0/11	123456	1236992	
0/12	--	--	
0/13	--	--	
0/14	--	--	
0/15	--	--	
0/16	--	--	
0/17	--	--	
0/18	--	--	
0/19	--	--	
0/20	--	--	
0/21	--	--	
0/22	--	--	
0/23	--	--	
0/24	--	--	

When the port has no flow shaping, it is displayed as --.

Edit

Edit Single Flow Shaping

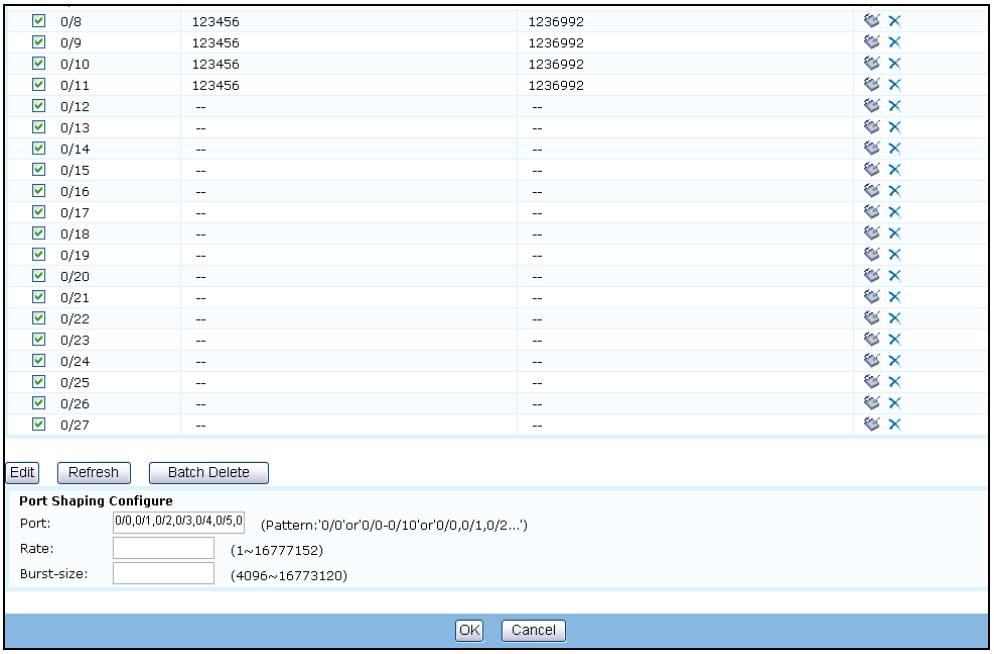
Click to configure the flow shaping of the port.



On the interface, there is the select port and the related values. The port cannot be modified.

Batch Edit

Click to edit the flow shaping of all selected ports.



On the interface, there are only the selected ports. You can also input the desired ports according to the port format.

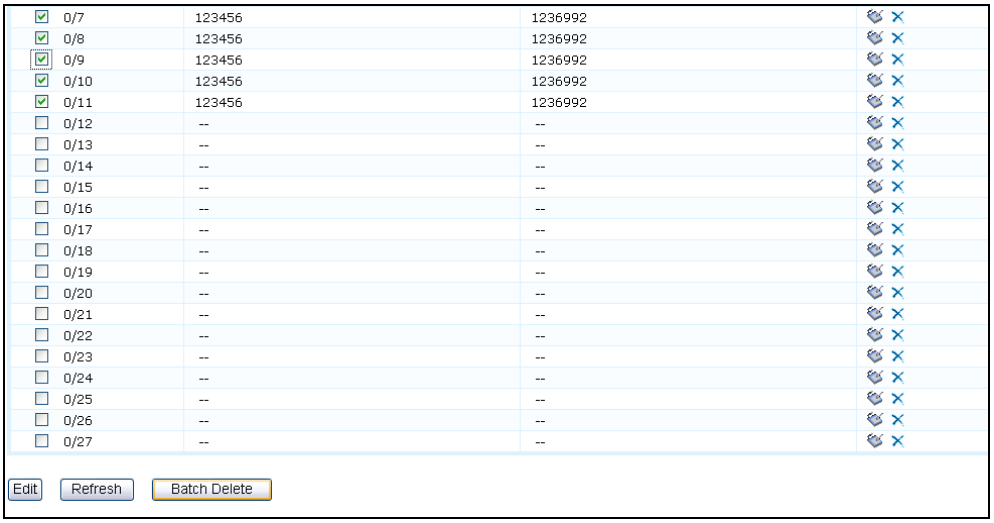
Delete

Delete Single Flow Shaping

Click ✕ to delete the flows shaping of the corresponding port.

Batch Delete

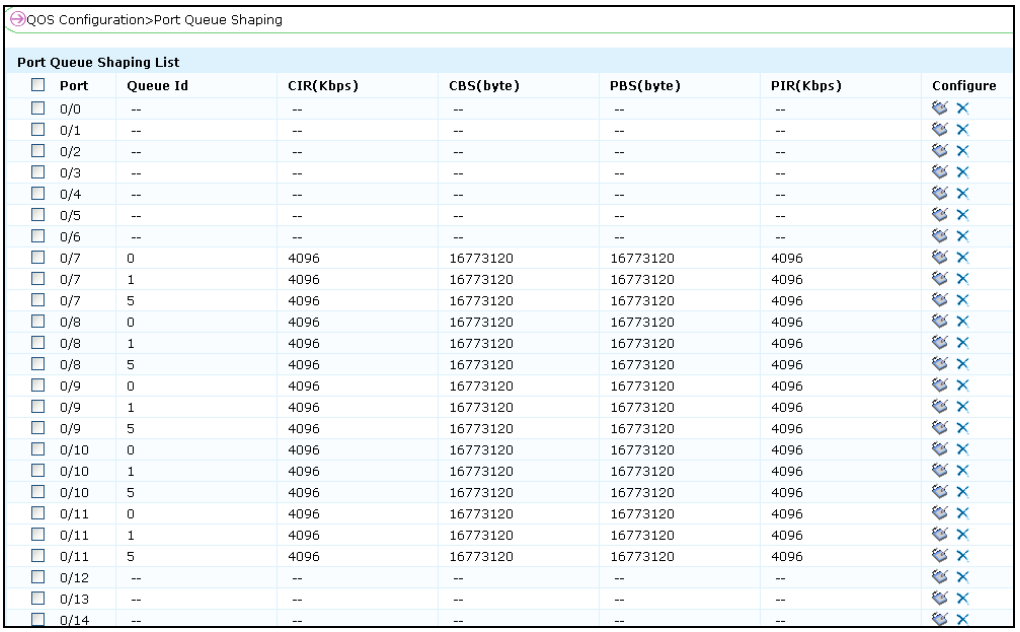
Click Batch Delete to delete the flow shaping of all selected ports.



Port Queue Flow Shaping

Port-based flow shaping at the output direction makes packets be sent out with even speed. The configured parameters are queue number, committed information rate, committed burst size, peak burst size, and peak information rate.

Configure the flow shaping for the queue on the port. The value range of the queue number is 0-7. The later four parameters are committed information rate (CIR), committed burst size (CBS), peak burst size (PBS), and peak information rate (PIR). Here, PIR, CIR and step length are all 64. If the input value is not the multiple of 64, the diver automatically adjusts it. The values of CBS and PBS are an integer multiple of 4096. The calculation method is consistent with the **burst-size** command.

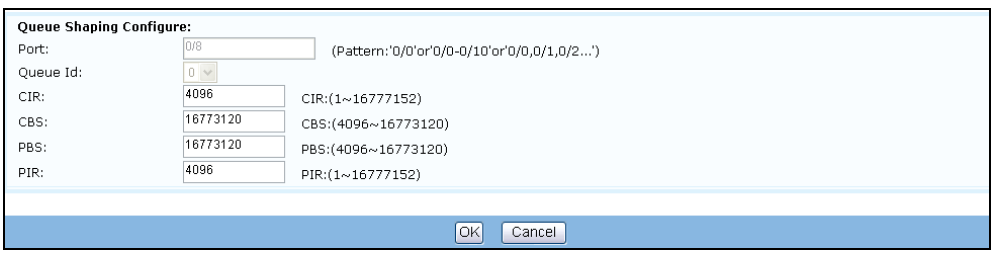


Port	Queue Id	CIR(Kbps)	CBS(byte)	PBS(byte)	PIR(Kbps)	Configure
0/0	--	--	--	--	--	
0/1	--	--	--	--	--	
0/2	--	--	--	--	--	
0/3	--	--	--	--	--	
0/4	--	--	--	--	--	
0/5	--	--	--	--	--	
0/6	--	--	--	--	--	
0/7	0	4096	16773120	16773120	4096	
0/7	1	4096	16773120	16773120	4096	
0/7	5	4096	16773120	16773120	4096	
0/8	0	4096	16773120	16773120	4096	
0/8	1	4096	16773120	16773120	4096	
0/8	5	4096	16773120	16773120	4096	
0/9	0	4096	16773120	16773120	4096	
0/9	1	4096	16773120	16773120	4096	
0/9	5	4096	16773120	16773120	4096	
0/10	0	4096	16773120	16773120	4096	
0/10	1	4096	16773120	16773120	4096	
0/10	5	4096	16773120	16773120	4096	
0/11	0	4096	16773120	16773120	4096	
0/11	1	4096	16773120	16773120	4096	
0/11	5	4096	16773120	16773120	4096	
0/12	--	--	--	--	--	
0/13	--	--	--	--	--	
0/14	--	--	--	--	--	

Edit

Edit Single Flow Shaping

Click to edit the flow shaping of the current queue number on the port.

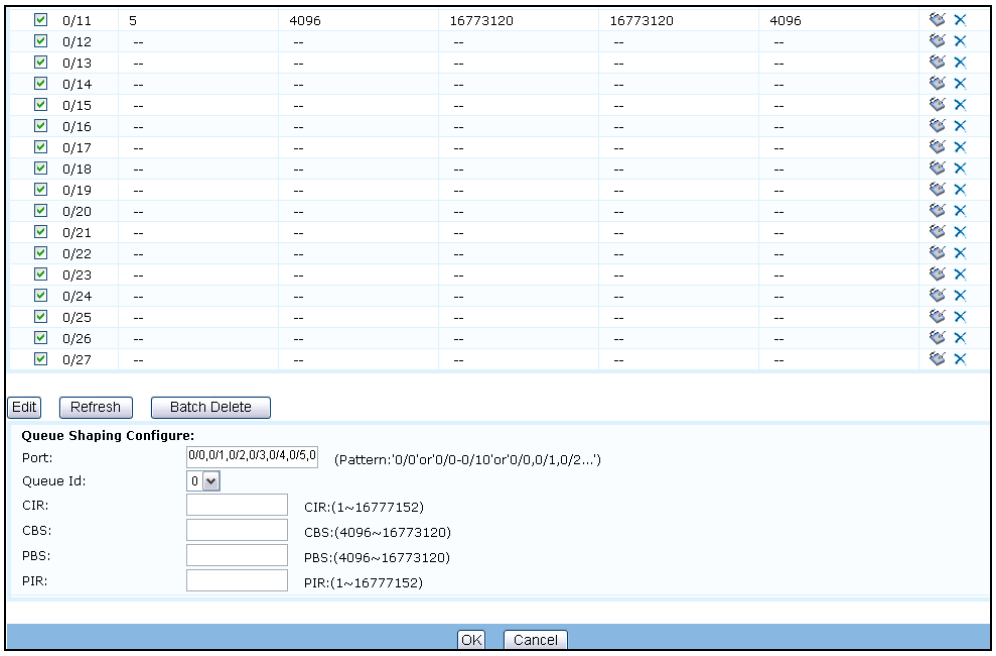


On the interface, there are the selected ports, queue ID, and the flow shaping values. Here, the selected ports and queue ID cannot be modified.

Batch Edit

Click

to edit the flow shaping of any queue number of all selected ports.



On the interface, there are only the select ports. Edit the flow shaping of one queue of the selected ports.

Delete

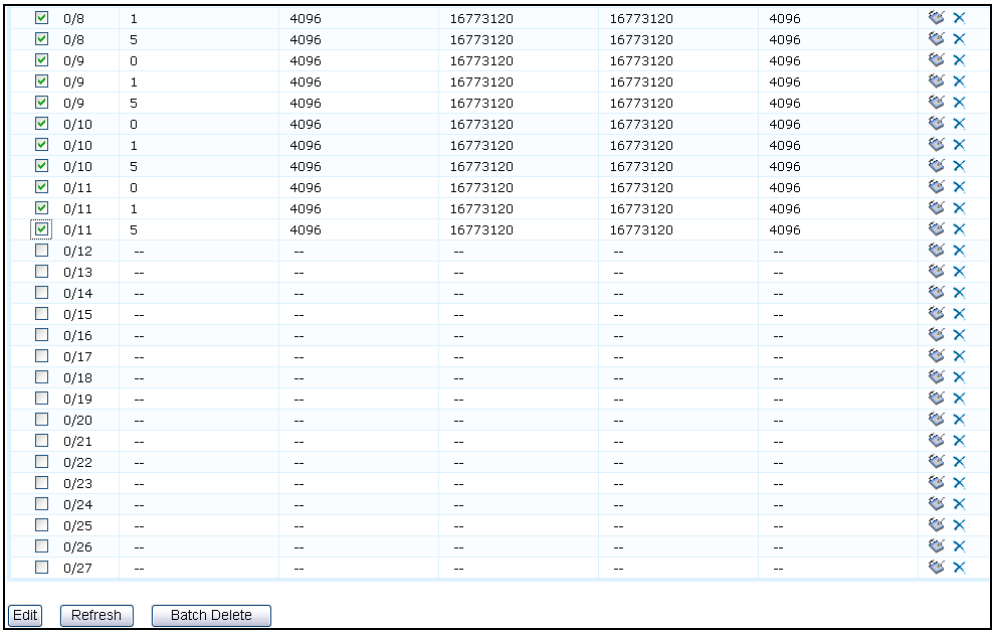
Delete Single Flow Shaping

Click to delete the flow shaping of current queue number on the port.

Batch Delete

Click

to delete the flow shaping of the selected queue numbers of the selected ports.



☑	0/8	1	4096	16773120	16773120	4096
☑	0/8	5	4096	16773120	16773120	4096
☑	0/9	0	4096	16773120	16773120	4096
☑	0/9	1	4096	16773120	16773120	4096
☑	0/9	5	4096	16773120	16773120	4096
☑	0/10	0	4096	16773120	16773120	4096
☑	0/10	1	4096	16773120	16773120	4096
☑	0/10	5	4096	16773120	16773120	4096
☑	0/11	0	4096	16773120	16773120	4096
☑	0/11	1	4096	16773120	16773120	4096
☑	0/11	5	4096	16773120	16773120	4096
☐	0/12	--	--	--	--	--
☐	0/13	--	--	--	--	--
☐	0/14	--	--	--	--	--
☐	0/15	--	--	--	--	--
☐	0/16	--	--	--	--	--
☐	0/17	--	--	--	--	--
☐	0/18	--	--	--	--	--
☐	0/19	--	--	--	--	--
☐	0/20	--	--	--	--	--
☐	0/21	--	--	--	--	--
☐	0/22	--	--	--	--	--
☐	0/23	--	--	--	--	--
☐	0/24	--	--	--	--	--
☐	0/25	--	--	--	--	--
☐	0/26	--	--	--	--	--
☐	0/27	--	--	--	--	--

Edit Refresh Batch Delete

The queue number and the corresponding flow shaping are deleted, but the port is not deleted. If there is no queue flow shaping on the port, it is displayed as --.

OAM Configuration

CFM Configuration

Overview

The IEEE 802.1ag protocol calls Ethernet OAM function as Connectivity Fault Management (CFM). It is service-based end-to-end Ethernet OAM function.

The carrier-class Ethernet needs to provide different management scope and contents for different organizations. Usually, there are three kinds of organizations that refer to carrier-class Ethernet services, including users, service providers, and network carriers. Users purchase Ethernet services from service providers; service providers can use their own network or other carriers' network to provide end-to-end Ethernet services. In IEEE 802.1ag, carrier-class Ethernet is divided to one multi-domain OAM network model, including three maintenance grades, that is, users, service providers, and carriers. They correspond to different management domains. The service providers are responsible for end-to-end service management and the carriers provide service transmission.

Maintenance Domain (MD): It is a part of the network covered by the connectivity fault management. Its limit is defined by a series of maintenance points (MP) configured on the ports. The maintenance domain name is used to identify the MD. According to multi-domain OAM network model of 802.1ag, MD has hierarchical levels. The high level can include the low level, but cannot intersect, that is, the range covered by high level is larger than that covered by the low level. The integers of 0-7 are used to identify different levels. The higher the level, the bigger the number.

Maintenance Association (MA): It is a set in MD and includes some MPs. MA is identified by MD name + short MA name. MA serves one VLAN, in which the packets sent by the MPs in MA are forwarded and the packets sent by other MPs in the MA are received at the same time. Therefore, MA is also called Service Instance (SI).

Maintenance point: It is one Maintenance Association End Point (MEP) or Maintenance Association Intermediate Point (MIP). It is configured on the port and belongs to one MA. On one port, each MA can be configured with only one MP.

Maintenance Association End Point (MEP): It can receive and send any CFM packet. Each MEP is identified by an integer, which is called MEP ID. MEP is configured on the port and decides the MD range. The MA and MD to which the MEP belongs decide the VLAN attribute and level attribute of the packet sent by MEP. According to the location of MEP in MA, the MEP direction includes inward and outward. If the packet in MA is received from the port on which the MEP is configured, the MEP direction is outward. Similarly, the outward MEP can only send packets to the network via the port on which the MEP is configured. Contrariwise, if the packet in MA is received from other port, the MEP direction is inward. The inward MEP cannot send packets to the network via the port on which the MEP is configured.

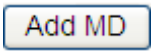
Maintenance Association Intermediate Point (MIP): It can process and respond to some CFM packets (such as LT packet or the packet whose destination is the LB which is at the same layer as itself), but cannot send packets initiatively. The MA and MD to which the MIP belongs decide the VLAN attribute and the MD level of the received packet.

CEM has the following functions:

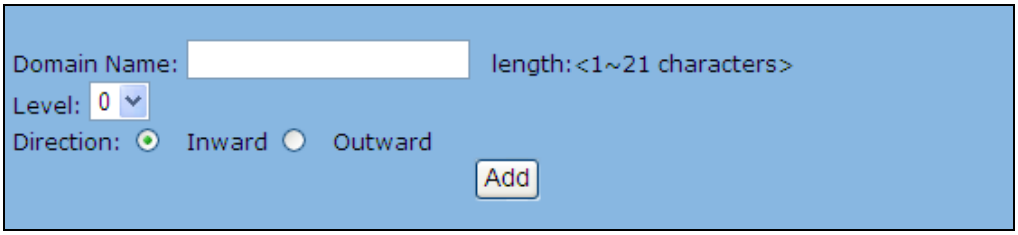
- The function of checking connectivity;
- The function of checking loopback;
- The function of tracking link;

Maintenance Domain Configuration

Add Maintenance Domain

Click 

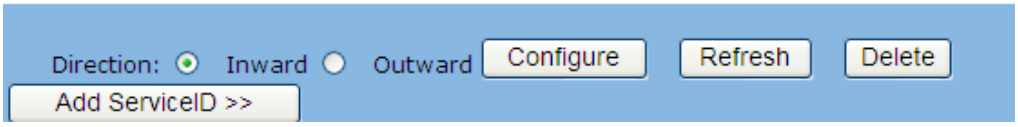
to enter into the interface for adding the maintenance domain.

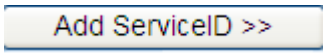


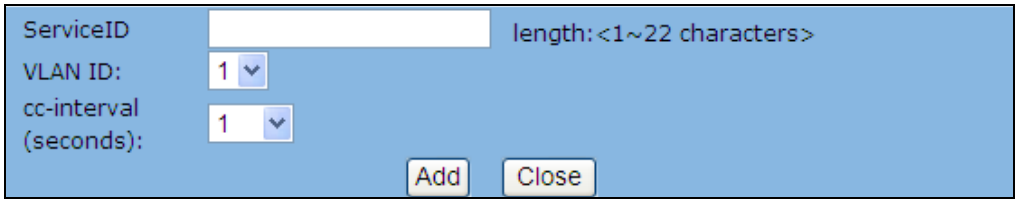
Add Service Instance of Maintenance Domain

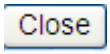
The initial interface of the maintenance domain is as follows:

Domain Name:	domain1
Level:	0
Direction:	Outward



Click  to enter into the interface for configuring the service instance.



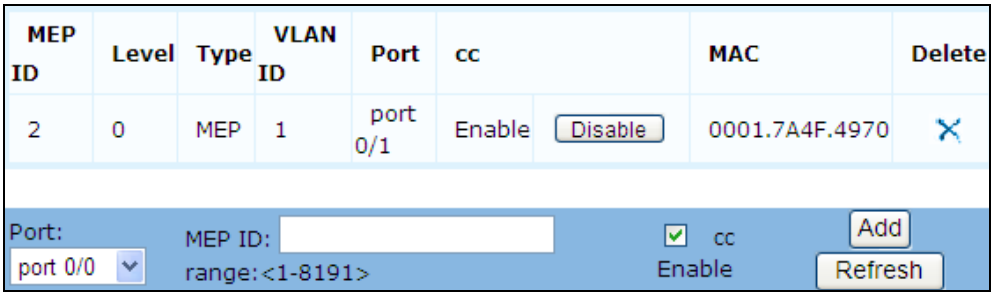
Click  to cancel adding the service instance of the maintenance domain.

The basic information of the service instance:

ServiceID	service1
VLAN ID:	1
Crosscheck:	Enable
cc-interval (seconds):	10
RDI:	Enable
Local-MEP:	1
Remote-MEP:	0
Crosscheck-MEP:	1

Click Configure to set the interval of MEP sending CCM packets; click Delete to delete the service instance.

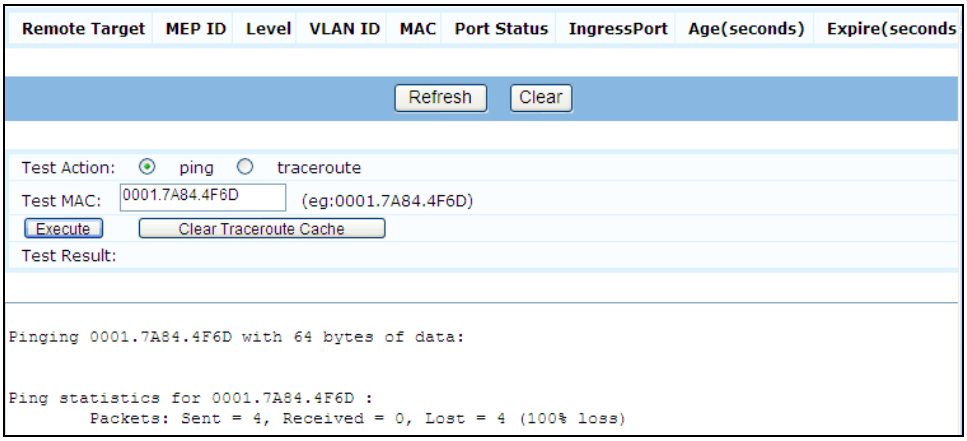
Local Maintenance End Point



Click Disable to disable the function of MEP sending CCM packets; click ✕ to delete the MEP.

Click Add to set the MEP on the port.

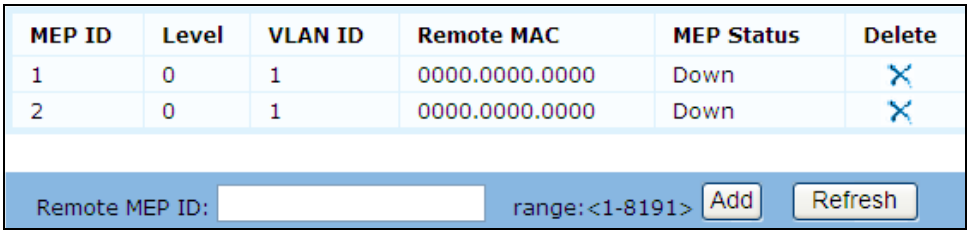
Remote Maintenance End Point



Action:

- Ping: loopback test;
- Traceroute: link tracking test;

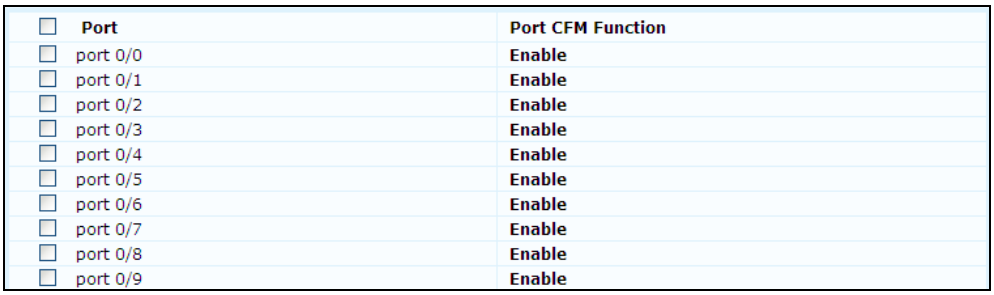
Connectivity Checking Maintenance End Point

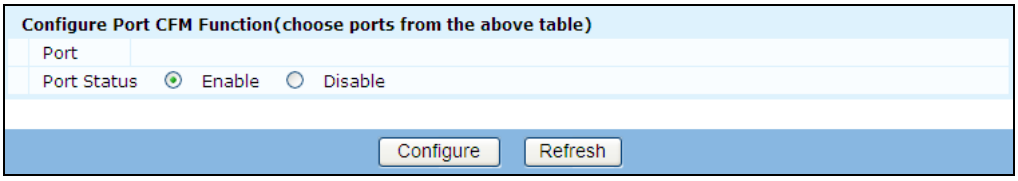


Click Add to add remote MEP; click ✕ to delete the remote MEP.

CFM Port Configuration

Configure the CFM function on the port.



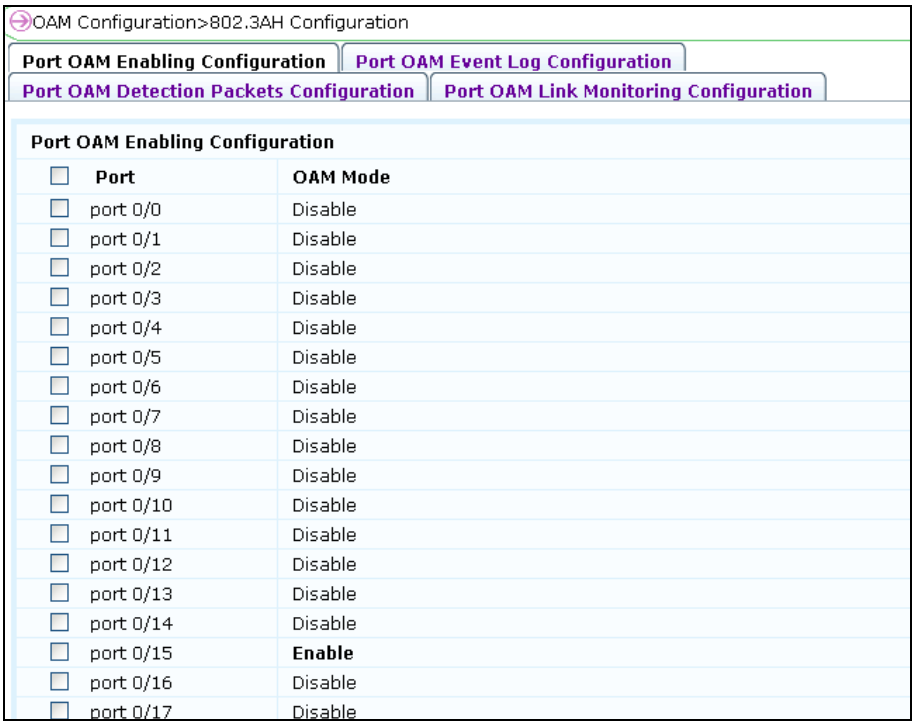


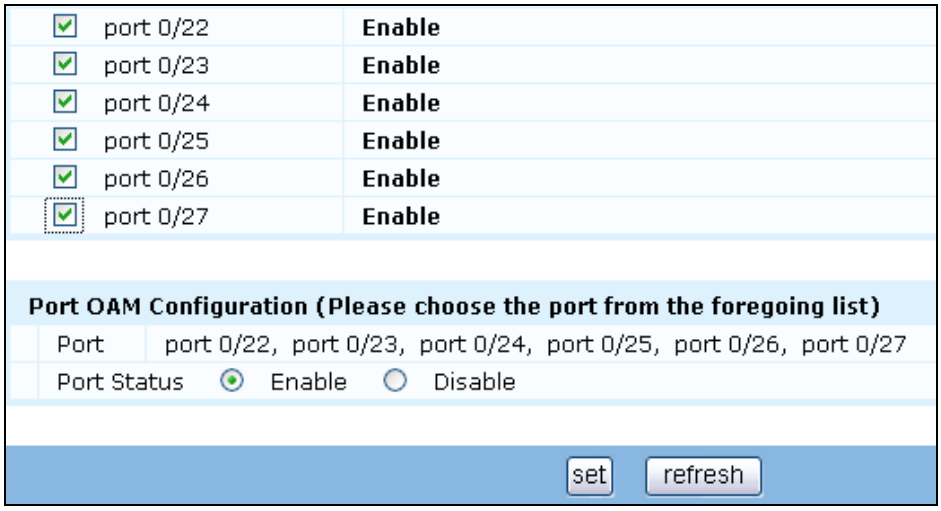
You can set whether to enable the CFM function on the ports in batches.

OAM Basic Configurations

This section describes the information about the Ethernet OAM. The interface includes four layers, that is, port OAM enabling configuration, port OAM event log configuration, port OAM detection packet configuration, and port OAM link monitoring configuration.

Port OAM Enabling Configuration

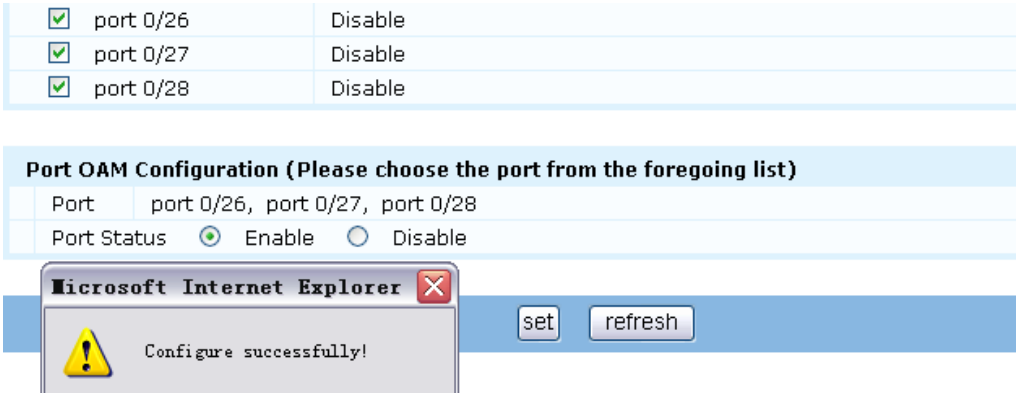


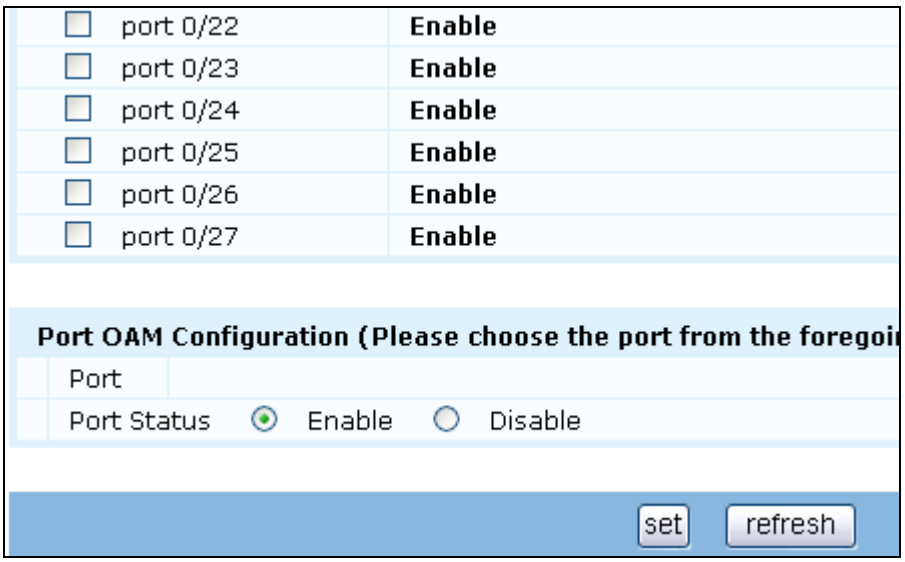


Port: the number of the port on which the OAM function is to be configured;

Port status: "Enable" means to enable the Ethernet OAM; "Disable" means to disable the Ethernet OAM; by default, the Ethernet OAM function is disabled.

Set: select the port number and the port status, and then click **Set**, as follows:





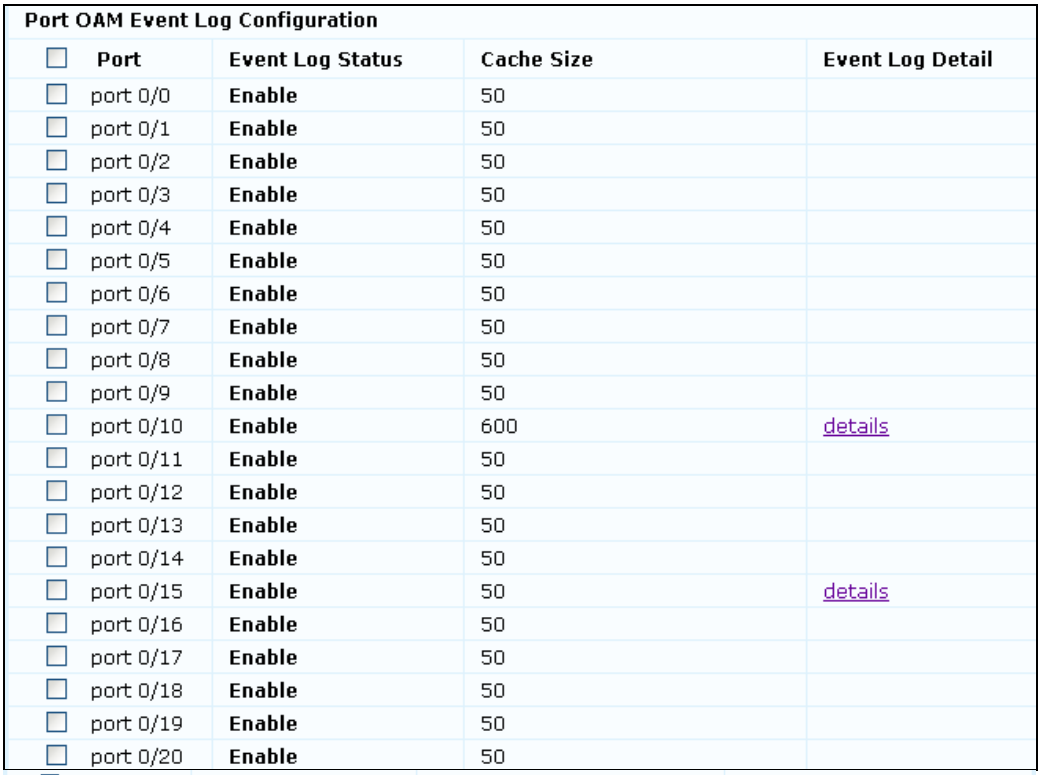
Note

After enabling the OAM function of the port, the OAM status in the list is displayed in the bold black form. Otherwise, it is not in bold form.

Refresh: Perform the refreshing operation on the interface.

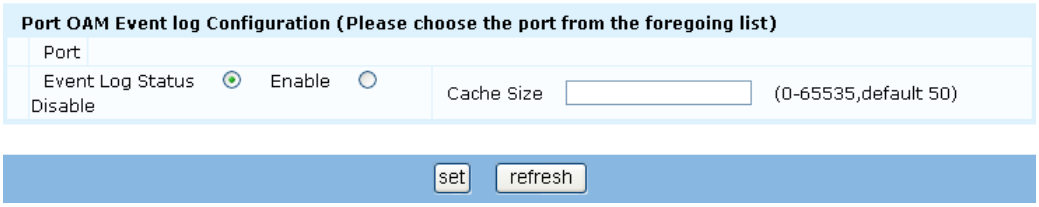
Port OAM Event Log Configuration

The following is the interface for configuring the OAM event log on the port.



Port OAM Event Log Configuration

Port	Event Log Status	Cache Size	Event Log Detail
port 0/0	Enable	50	
port 0/1	Enable	50	
port 0/2	Enable	50	
port 0/3	Enable	50	
port 0/4	Enable	50	
port 0/5	Enable	50	
port 0/6	Enable	50	
port 0/7	Enable	50	
port 0/8	Enable	50	
port 0/9	Enable	50	
port 0/10	Enable	600	details
port 0/11	Enable	50	
port 0/12	Enable	50	
port 0/13	Enable	50	
port 0/14	Enable	50	
port 0/15	Enable	50	details
port 0/16	Enable	50	
port 0/17	Enable	50	
port 0/18	Enable	50	
port 0/19	Enable	50	
port 0/20	Enable	50	
port 0/2/21	Disable	111	details
port 0/2/22	Disable	111	details
port 0/2/23	Disable	111	details



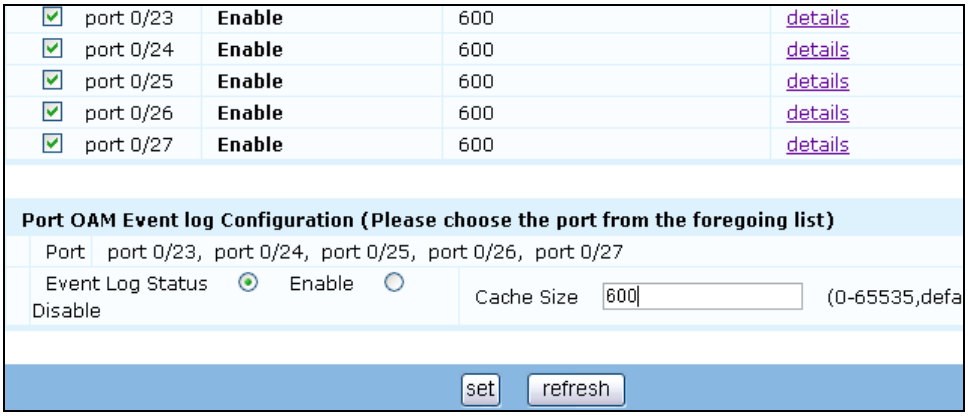
Port: the number of the port on which the OAM event log is to be configured;

Event Log Status: “Enable” means to enable the event log information; “Disable” means to disable the event log information; by default, the event log information is enabled;

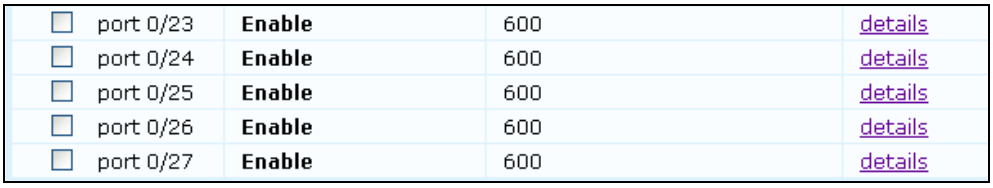
Cache Size: the maximum number of the cached event log information of the Ethernet OAM; the default value is 50;

Event Log Detail: When the port is configured with the maximum cache size, there is the link of the details. Click **Detail** to display the detailed information as follows. Click **Close** to hide the information.

Set: Select port number, event log status, and cache size, and then click **Set** as follows.



After setting successfully, the following figure is displayed.

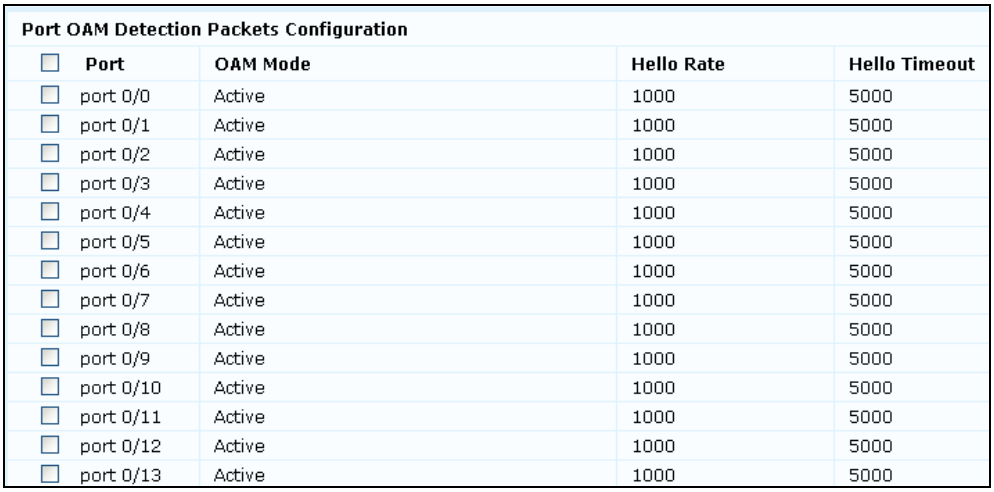


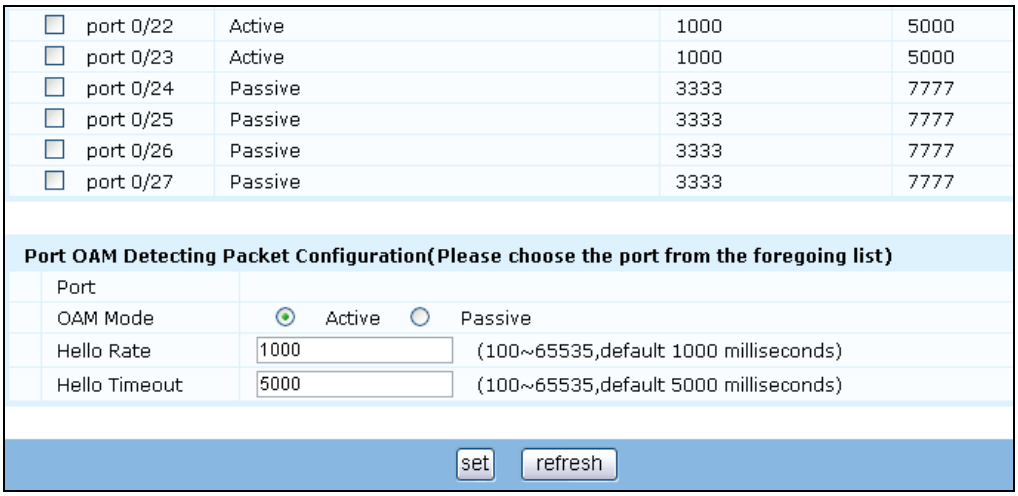
🕮 Note

After enabling the OAM event log of the port, the event log status in the list is displayed in the bold black form. Otherwise, it is not in bold form.

Port OAM Detection Packet Configuration

The following is the interface for configuring the OAM detection packet.





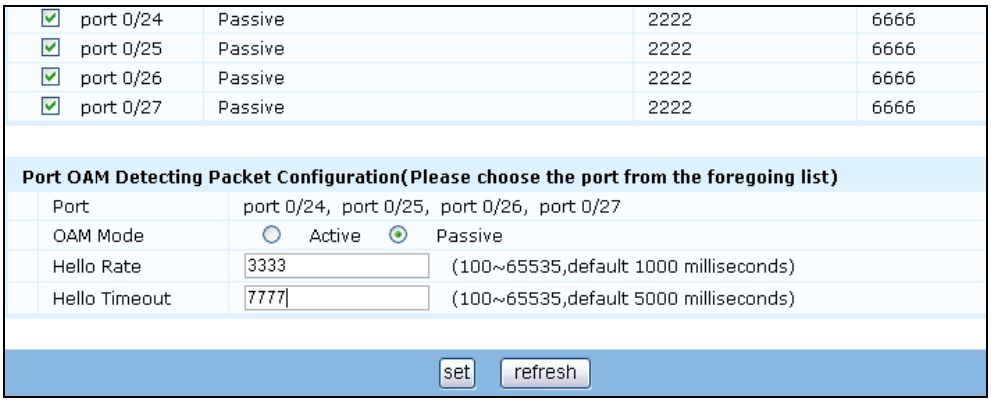
Port: the number of the port on which the OAM detection packet is configured;

OAM Mode: It is the Ethernet OAM mode. “Active” means the Ethernet OAM mode is active; “Passive” means the Ethernet OAM mode is passive. The default value is active.

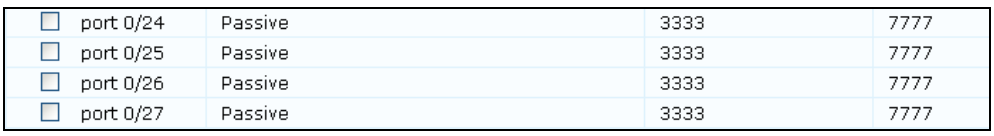
Hello rate: It is the interval for sending hello packets (that is information OAMPDU) of Ethernet OAM. The default value is 1000.

Hello Timeout: It is the timeout of the Ethernet OAM connection. The default value is 5000;

Set: Select the port number, OAM mode, Hello rate, and Hello timeout, and then click **Set** as follows.



After setting successfully, the following interface is displayed.



Refresh: Perform the refreshing operation on the interface.

Port OAM Link Monitoring Configuration

The following is the interface for configuring OAM link monitoring on the port.

Port OAM Link Monitoring Configuration

Port	Link Monitor Status	Monitor Error Symbol			Monitor Error Frame			Monitor Error Frame Period			Monitor Error Fra	
		Window (seconds)	High Threshold Value And Action	Low Threshold Value And Action	Window (seconds)	High Threshold Value And Action	Low Threshold Value And Action	Window (seconds)	High Threshold Value And Action	Low Threshold Value And Action	Window (seconds)	High Threshol Value An Action
port 0/0	Enable	1	No Monitor	1 : None	1	No Monitor	1 : None	1000	No Monitor	1 : None	60	No Monitor
port 0/1	Enable	1	No Monitor	1 : None	1	No Monitor	1 : None	1000	No Monitor	1 : None	60	No Monitor
port 0/2	Enable	1	No Monitor	1 : None	1	No Monitor	1 : None	1000	No Monitor	1 : None	60	No Monitor
port 0/3	Enable	1	No Monitor	1 : None	1	No Monitor	1 : None	1000	No Monitor	1 : None	60	No Monitor
port 0/4	Enable	1	No Monitor	1 : None	1	No Monitor	1 : None	1000	No Monitor	1 : None	60	No Monitor
port 0/5	Enable	1	No Monitor	1 : None	1	No Monitor	1 : None	1000	No Monitor	1 : None	60	No Monitor

Port: the number of the port on which the OAM link monitoring is to be configured;

Link monitor status: the link monitoring function of Ethernet OAM; “Enable” means to enable the link monitoring function of Ethernet OAM; “Disable” means to disable the link monitoring function of Ethernet OAM; by default, the link monitoring function of Ethernet OAM is enabled;

Window (seconds) of monitor error symbol: the window period of the error signal detection of the OAM link monitoring; the default value is 1s;

High threshold value and action: the upper threshold of the error signal detection of Ethernet OAM link monitoring and the error response processing for the upper threshold of the error signal detection of Ethernet OAM link monitoring; by default, the upper threshold is no monitor;

Low threshold value and action: the low threshold of the error signal detection of Ethernet OAM link monitoring and the error response processing for the low threshold of the error signal detection of Ethernet OAM link monitoring; by default, the low threshold is 1;

Window (seconds) of monitor error frame: the window period of the error frame detection of Ethernet OAM link monitoring; the default value is 1 second;

High threshold value and action: the upper threshold of the error frame detection of Ethernet OAM link monitoring and the error response processing for the upper threshold of the error frame detection of Ethernet OAM link monitoring; the default upper threshold value is no monitor;

Low threshold value and action: the low threshold of the error frame detection of Ethernet OAM link monitoring and the error response processing for the low threshold of the error frame detection of Ethernet OAM link monitoring; the default low threshold is 1;

Window (seconds) of monitor error frame period: the window period of the error frame periodical detection of Ethernet OAM link monitoring; the default value is 1000 frames;

High threshold value and action: the upper threshold of the error frame periodical detection of Ethernet OAM link monitoring and the error response processing for the upper threshold of the error frame periodical detection of Ethernet OAM link monitoring; the default upper threshold value is no monitor;

Low threshold value and action: the low threshold of the error frame periodical detection of Ethernet OAM link monitoring and the error response processing for the low threshold of the error frame periodical detection of Ethernet OAM link monitoring; the default low threshold is 1;

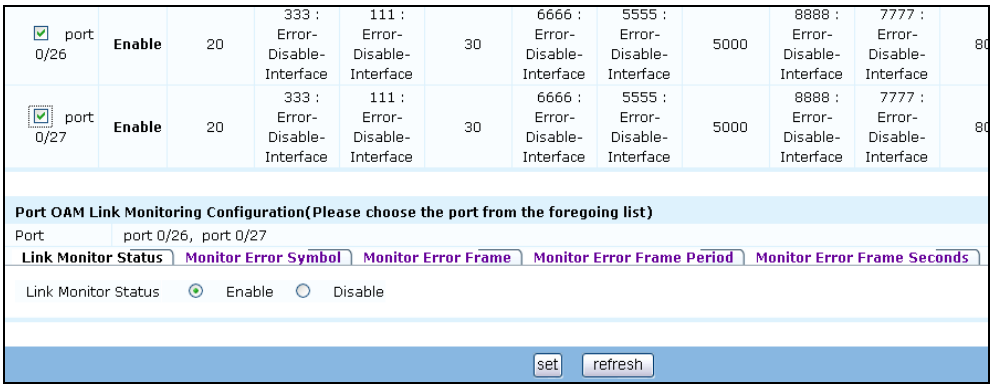
Window (seconds) of monitor error frame seconds: the window period of the error frame seconds detection of Ethernet OAM link monitoring; the default value is 60s.

High threshold value and action: the upper threshold of the error frame seconds detection of Ethernet OAM link monitoring and the error response processing for the upper threshold of the error frame seconds detection of Ethernet OAM link monitoring; the default upper threshold value is no monitor;

Low threshold value and action: the low threshold of the error frame seconds detection of Ethernet OAM link monitoring and the error response processing for the low threshold of the error frame seconds detection of Ethernet OAM link monitoring; the default low threshold is 1;

The setting list includes Link Monitor Status, Monitor Error Symbol, Monitor Error Frame, Monitor Error Frame Period, and Monitor Error Frame Seconds.

The setting of link monitoring status is as follows:



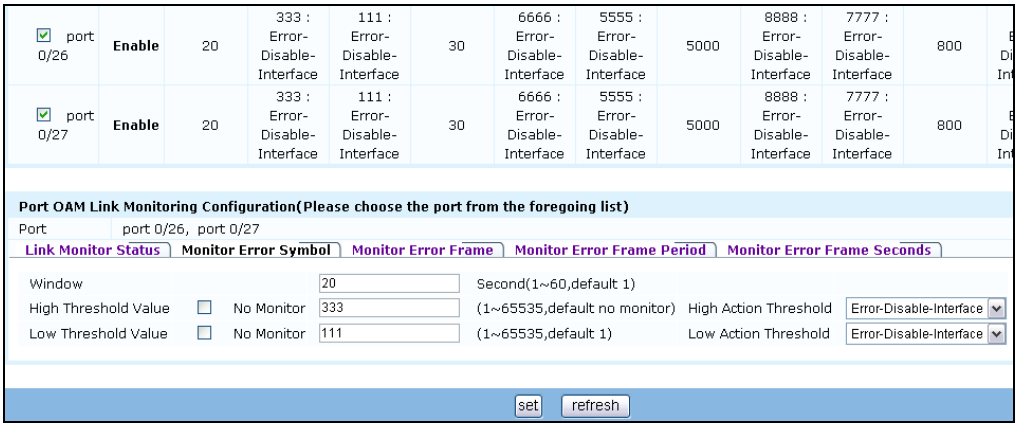
The selected port numbers are automatically added to the port list. After successful setting, the following interface is shown.

port 0/26	**Enable**	20	333 : Error-Disable-Interface	111 : Error-Disable-Interface	30
port 0/27	**Enable**	20	333 : Error-Disable-Interface	111 : Error-Disable-Interface	30

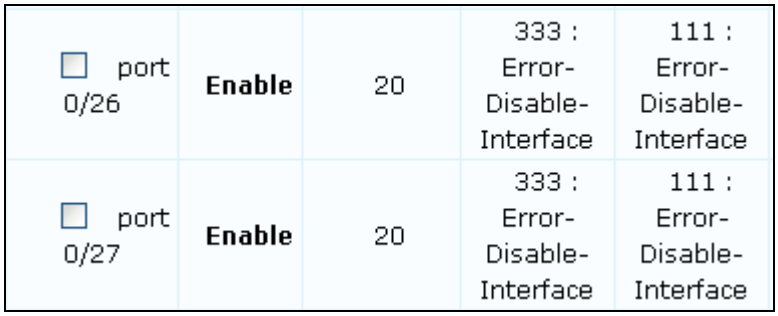
📖 Note

After enabling OAM link monitoring configuration on the port, the link monitoring status in the list is displayed in bold and black form. Otherwise, it is displayed not in bold form.

The setting of the error signal detection is as follows:

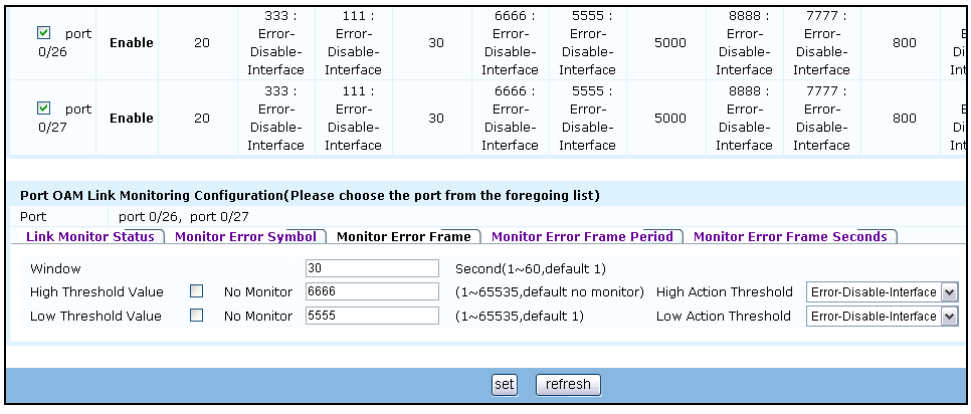


After successful setting, the following interface is shown.



Refresh: to refresh the interface;

The setting of the error frame detection is as follows:

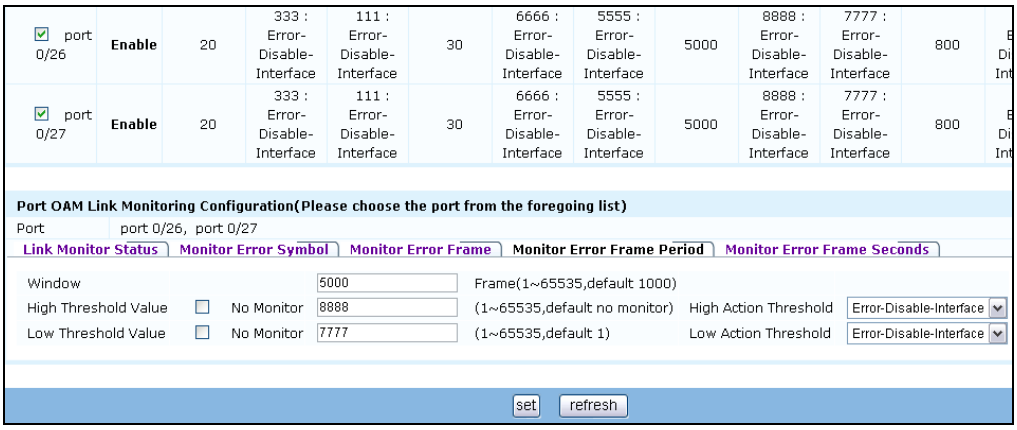


After successful setting, the following interface is shown.

port 0/26	**Enable**	20	333 : Error-Disable-Interface	111 : Error-Disable-Interface	30	6666 : Error-Disable-Interface	5555 : Error-Disable-Interface
port 0/27	**Enable**	20	333 : Error-Disable-Interface	111 : Error-Disable-Interface	30	6666 : Error-Disable-Interface	5555 : Error-Disable-Interface

Refresh: to refresh the interface;

The setting of the error frame periodical detection is as follows:

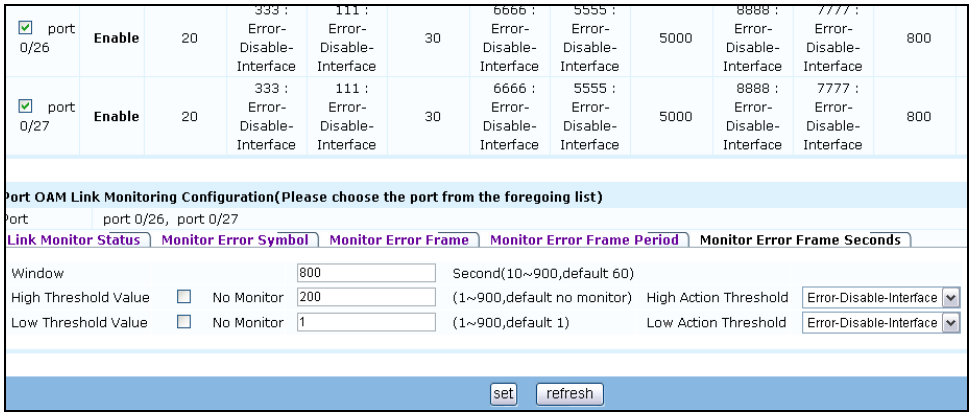


After successful setting, the following interface is shown.

port 0/26	**Enable**	20	333 : Error-Disable-Interface	111 : Error-Disable-Interface	30	6666 : Error-Disable-Interface	5555 : Error-Disable-Interface	5000	8888 : Error-Disable-Interface	7777 : Error-Disable-Interface
port 0/27	**Enable**	20	333 : Error-Disable-Interface	111 : Error-Disable-Interface	30	6666 : Error-Disable-Interface	5555 : Error-Disable-Interface	5000	8888 : Error-Disable-Interface	7777 : Error-Disable-Interface

Refresh: to refresh the interface;

The setting of the error frame seconds detection is as follows:



After successful setting, the following interface is shown.

30	6666 : Error-Disable-Interface	5555 : Error-Disable-Interface	5000	8888 : Error-Disable-Interface	7777 : Error-Disable-Interface	800	200 : Error-Disable-Interface	1 : Error-Disable-Interface
30	6666 : Error-Disable-Interface	5555 : Error-Disable-Interface	5000	8888 : Error-Disable-Interface	7777 : Error-Disable-Interface	800	200 : Error-Disable-Interface	1 : Error-Disable-Interface

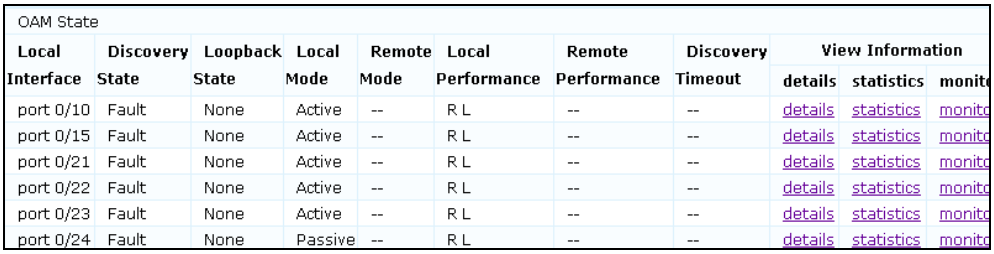
Refresh: to refresh the interface;

📖 Note

The interface comprises tabs. When the user sets one tab, the setting takes effect only on the current tab. For example, select **Monitor Error Frame Seconds**, click **Set** and the setting takes effect only on the tab.

OAM Status Display

This section describes the display information of Ethernet OAM status.



Details: to display the discovery information of Ethernet OAM connection, as follows:

Port port 0/10			
Local Client			
Operational Status			
Link Type	port	**Link Index**	11
Hardware State	down	**OAM Enable**	disable
Hello Rate	1000msec	**Hello Timeout**	5000msec
Link State	fault	**Link State On Time**	02:31:39
Loopback State	none	**Multiplexer Mode**	forward
Parser Mode	forward	**Next Hello In**	none
Timeout In	none		
Information OAMPDU			
Critical Link Events	none	**Local Stable**	
Remote Stable		**OAM Version**	1
Reversion	0	**Parser State**	forward
Multiplexer State	forward	**Mode**	active
Capability	r l	**MTU Size**	1500
Vendor ID(oui)	0x00 0x01 0x7a (maipu)	**Vendor Specific**	0x00 0x00 0x00 0x00
Remote Client			
Operational Status			
MAC address			

Remote Client			
Operational Status			
MAC address			
Information OAMPDU			
Critical Link Events		**Local Stable**	
Remote Stable		**OAM Version**	
Revision		**Parser State**	
Multiplexer State		**Mode**	
Capability		**MTU Size**	
Vendor ID (oui)		**Vendor Specific**	
			close

Close: to close the list of displaying the details;

Statistics: to display the statistics information of Ethernet OAM, as follows:

Port port 0/3			
OAMPDU Packet Counter			
Information OAM Tx/Rx/Err	60/0/0	Unique Event Notification OAMPDU Tx/Rx/Err	0/0/0
Duplicate Event Notification OAMPDU Tx/Rx/Err	0/0/0	Loopback Control OAMPDU Tx/Rx/Err	0/0/0
Variable Request OAMPDU Tx/Rx/Err	0/0/0	Variable Response OAMPDU Tx/Rx/Err	0/0/0
Organization Specific OAMPDU Tx/Rx/Err	0/0/0	Unsupported OAMPDU Tx/Rx/Err	0/0/0
Frames Lost Due To Ethernet OAM Multiplexer	0		
Local Link Event Counter			
Link Fault	0	Dying Gasp	0
Critical Event	0	Errored Symbol	0
Errored Frame	0	Errored Frame-Period	0
Errored Frame-Seconds	0		
Remote Link Event Counter			
Link Fault	0	Dying Gasp	0
Critical Event	0	Errored Symbol	0
Errored Frame	0	Errored Frame-Period	0
Errored Frame-Seconds	0		
close			

Close: to close the list of displaying the statistics information;

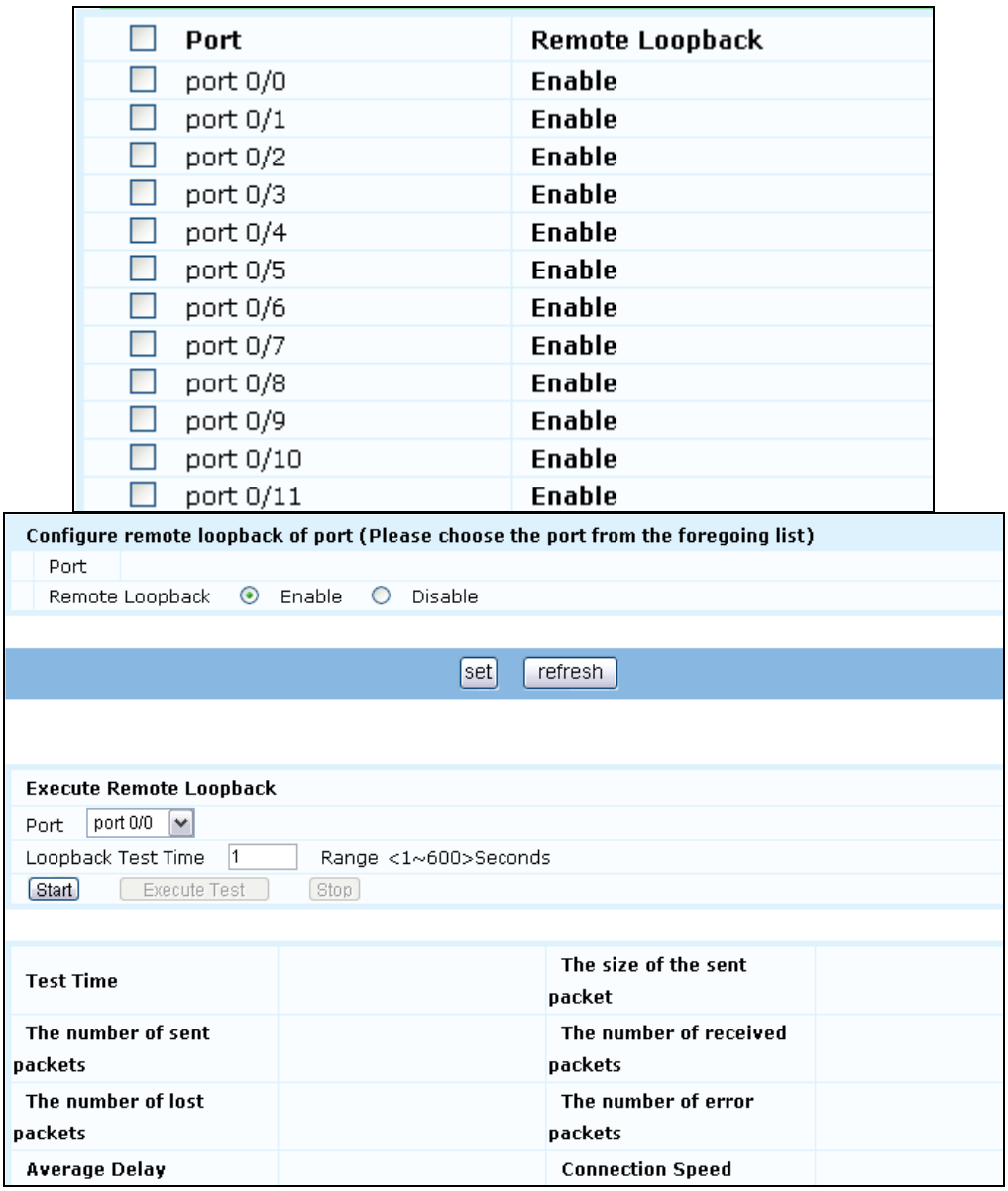
Monitor: to display the Ethernet OAM link monitoring information, as follows.

Link Monitor Error Frame Event Check			
Window Size	1 x 1 seconds	Threshold Low Value	1
Threshold Low Action	none	Threshold High Value	none
Threshold High Action	none	Last Error Number	0
Next Error Check In	none	Error Statistics	0
Link Monitor Error Frame-Period Event Check			
Window Size	1000 x 10,000 frames	Threshold Low Value	1
Threshold Low Action	none	Threshold High Value	none
Threshold High Action	none	Last Error Number	0
Next Error Check In	none	Error Statistics	0
Link Monitor Error Frame-Seconds Event Check			
Window Size	60 x 1 seconds	Threshold Low Value	1
Threshold Low Action	none	Threshold High Value	none
Threshold High Action	none	Last Error Number	0
Next Error Check In	none	Error Statistics	0
close			

Close: to close the list of displaying Ethernet OAM link monitoring information;

OAM Remote Loopback Test

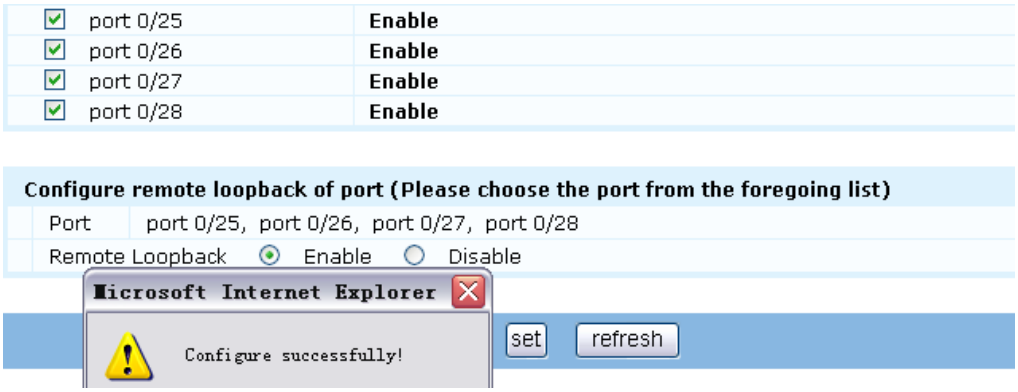
This section describes the remote loopback test information of the Ethernet OAM.



Port: the number of the port to be configured with OAM remote loopback test;

Remote Loopback: The remote loopback function of Ethernet OAM; "**Enable**" means that the remote loopback function of Ethernet OAM is not disabled; "**Disable**" means that the remote loopback function of Ethernet OAM is disabled; the default value is "**Enable**".

The setting is as follows:

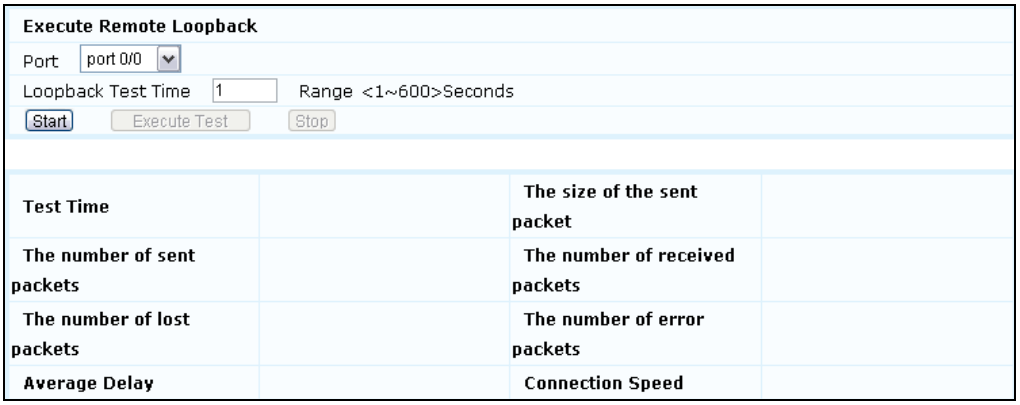


After setting successfully, the following interface is shown.

📖 Note

After enabling the OAM remote loopback test function on the port, the remote loopback function in the list is displayed in black and bold form. Otherwise, it is displayed not in bold form.

Refresh: to refresh the interface;



Port: the number of the port to send the remote loopback command;

Loopback Test Time: the time of the remote loopback test; the unit is second;

Start: to send the command of enabling remote loopback test to the peer end;

Execute Test: After enabling the remote loopback command, click **Execute Test**, and then the tested data is displayed on the interface;

Stop: to send the command of disabling remote loopback test to the peer end;

ELMI Configuration

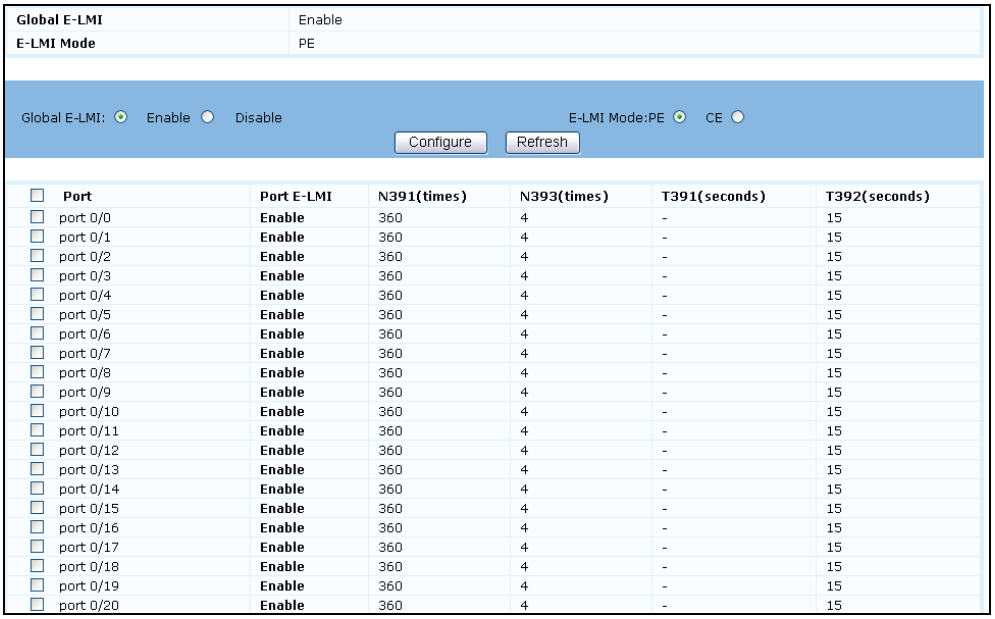
E-LMI (Ethernet local management interface) is put forward by MEF and the serial No. is MEF16. Metro-E forum defines a group of extending service attributes and related parameters used to provide the Ethernet services from UNI to UNI. The E-LMI protocol can get and transmit the sufficient EVC and UNI status information, and UNI and EVC configuration information from the PE device to the CE device, so as to complete the configuration of the CE device.

Port	Port E-LMI	N391(times)	N393(times)	T391(seconds)	T392(seconds)
port 0/0	Enable	360	4	-	15
port 0/1	Enable	360	4	-	15
port 0/2	Enable	360	4	-	15
port 0/3	Enable	360	4	-	15
port 0/4	Enable	360	4	-	15
port 0/5	Enable	360	4	-	15
port 0/6	Enable	360	4	-	15
port 0/7	Enable	360	4	-	15
port 0/8	Enable	360	4	-	15
port 0/9	Enable	360	4	-	15
port 0/10	Enable	360	4	-	15
port 0/11	Enable	360	4	-	15
port 0/12	Enable	360	4	-	15
port 0/13	Enable	360	4	-	15
port 0/14	Enable	360	4	-	15
port 0/15	Enable	360	4	-	15
port 0/16	Enable	360	4	-	15
port 0/17	Enable	360	4	-	15
port 0/18	Enable	360	4	-	15
port 0/19	Enable	360	4	-	15
port 0/20	Enable	360	4	-	15
port 0/21	Enable	360	4	-	15
port 0/22	Enable	360	4	-	15
port 0/23	Enable	360	4	-	15
port 0/24	Enable	360	4	-	15
port 0/25	Enable	360	4	-	15
port 0/26	Enable	360	4	-	15
port 0/27	Enable	360	4	-	15
link-aggregation 2	Enable	360	4	-	15
link-aggregation 3	Enable	360	4	-	15
link-aggregation 4	Enable	360	4	-	15
link-aggregation 5	Enable	360	4	-	15

E-LMI Protocol Configuration on PE

Global E-LMI Function

Select Global E-LMI: Enable and E-LMI Mode:PE CE, and then click **Set**.



Global E-LMI	Enable
E-LMI Mode	PE

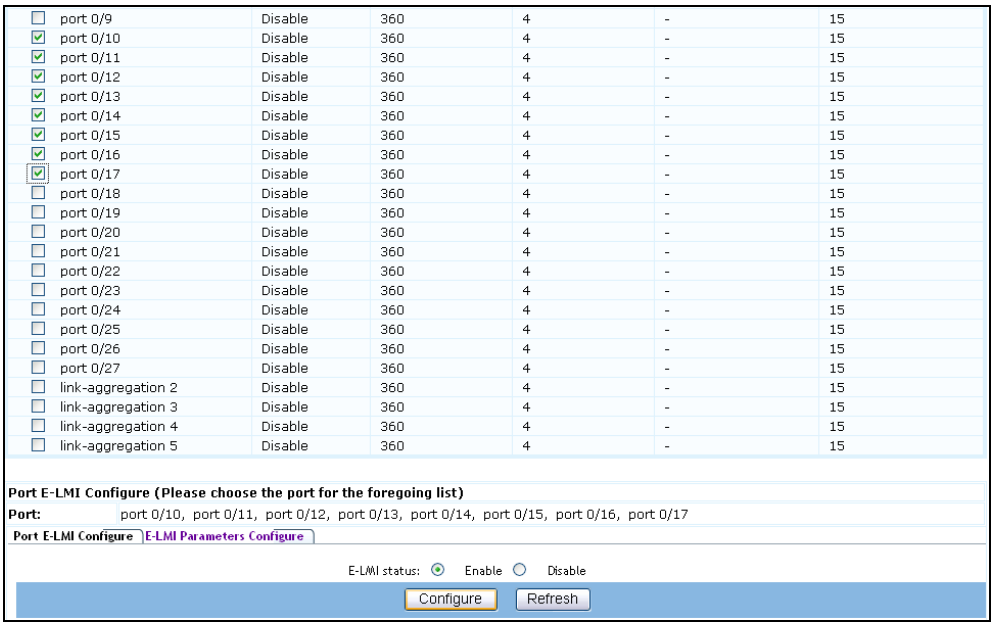
Global E-LMI: Enable Disable E-LMI Mode:PE CE

Configure Refresh

Port	Port E-LMI	N391(times)	N393(times)	T391(seconds)	T392(seconds)
port 0/0	Enable	360	4	-	15
port 0/1	Enable	360	4	-	15
port 0/2	Enable	360	4	-	15
port 0/3	Enable	360	4	-	15
port 0/4	Enable	360	4	-	15
port 0/5	Enable	360	4	-	15
port 0/6	Enable	360	4	-	15
port 0/7	Enable	360	4	-	15
port 0/8	Enable	360	4	-	15
port 0/9	Enable	360	4	-	15
port 0/10	Enable	360	4	-	15
port 0/11	Enable	360	4	-	15
port 0/12	Enable	360	4	-	15
port 0/13	Enable	360	4	-	15
port 0/14	Enable	360	4	-	15
port 0/15	Enable	360	4	-	15
port 0/16	Enable	360	4	-	15
port 0/17	Enable	360	4	-	15
port 0/18	Enable	360	4	-	15
port 0/19	Enable	360	4	-	15
port 0/20	Enable	360	4	-	15

Enable E-LMI on Port

Select the port, select E-LMI status: Enable Disable, and then click **Set**.



port 0/9	Disable	360	4	-	15
port 0/10	Disable	360	4	-	15
port 0/11	Disable	360	4	-	15
port 0/12	Disable	360	4	-	15
port 0/13	Disable	360	4	-	15
port 0/14	Disable	360	4	-	15
port 0/15	Disable	360	4	-	15
port 0/16	Disable	360	4	-	15
port 0/17	Disable	360	4	-	15
port 0/18	Disable	360	4	-	15
port 0/19	Disable	360	4	-	15
port 0/20	Disable	360	4	-	15
port 0/21	Disable	360	4	-	15
port 0/22	Disable	360	4	-	15
port 0/23	Disable	360	4	-	15
port 0/24	Disable	360	4	-	15
port 0/25	Disable	360	4	-	15
port 0/26	Disable	360	4	-	15
port 0/27	Disable	360	4	-	15
link-aggregation 2	Disable	360	4	-	15
link-aggregation 3	Disable	360	4	-	15
link-aggregation 4	Disable	360	4	-	15
link-aggregation 5	Disable	360	4	-	15

Port E-LMI Configure (Please choose the port for the foregoing list)

Port: port 0/10, port 0/11, port 0/12, port 0/13, port 0/14, port 0/15, port 0/16, port 0/17

Port E-LMI Configure | E-LMI Parameters Configure

E-LMI status: Enable Disable

Configure Refresh

The result is as follows:

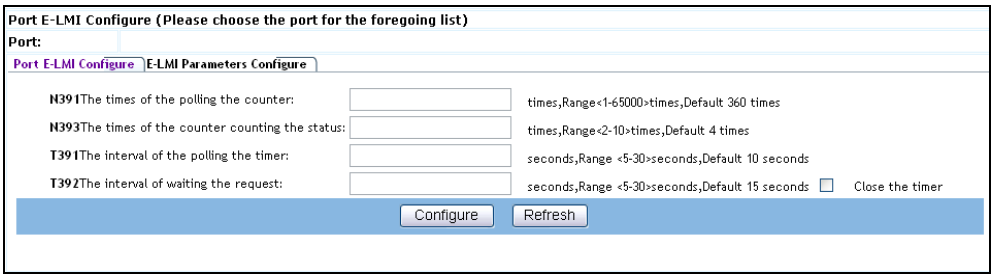
Port	Port E-LMI	N391(times)	N393(times)	T391(seconds)	T392(seconds)
port 0/0	Disable	360	4	-	15
port 0/1	Disable	360	4	-	15
port 0/2	Disable	360	4	-	15
port 0/3	Disable	360	4	-	15
port 0/4	Disable	360	4	-	15
port 0/5	Disable	360	4	-	15
port 0/6	Disable	360	4	-	15
port 0/7	Disable	360	4	-	15
port 0/8	Disable	360	4	-	15
port 0/9	Disable	360	4	-	15
port 0/10	**Enable**	360	4	-	15
port 0/11	**Enable**	360	4	-	15
port 0/12	**Enable**	360	4	-	15
port 0/13	**Enable**	360	4	-	15
port 0/14	**Enable**	360	4	-	15
port 0/15	**Enable**	360	4	-	15
port 0/16	**Enable**	360	4	-	15
port 0/17	**Enable**	360	4	-	15
port 0/18	Disable	360	4	-	15
port 0/19	Disable	360	4	-	15
port 0/20	Disable	360	4	-	15
port 0/21	Disable	360	4	-	15
port 0/22	Disable	360	4	-	15
port 0/23	Disable	360	4	-	15
port 0/24	Disable	360	4	-	15
port 0/25	Disable	360	4	-	15
port 0/26	Disable	360	4	-	15
port 0/27	Disable	360	4	-	15
link-aggregation 2	Disable	360	4	-	15
link-aggregation 3	Disable	360	4	-	15
link-aggregation 4	Disable	360	4	-	15
link-aggregation 5	Disable	360	4	-	15

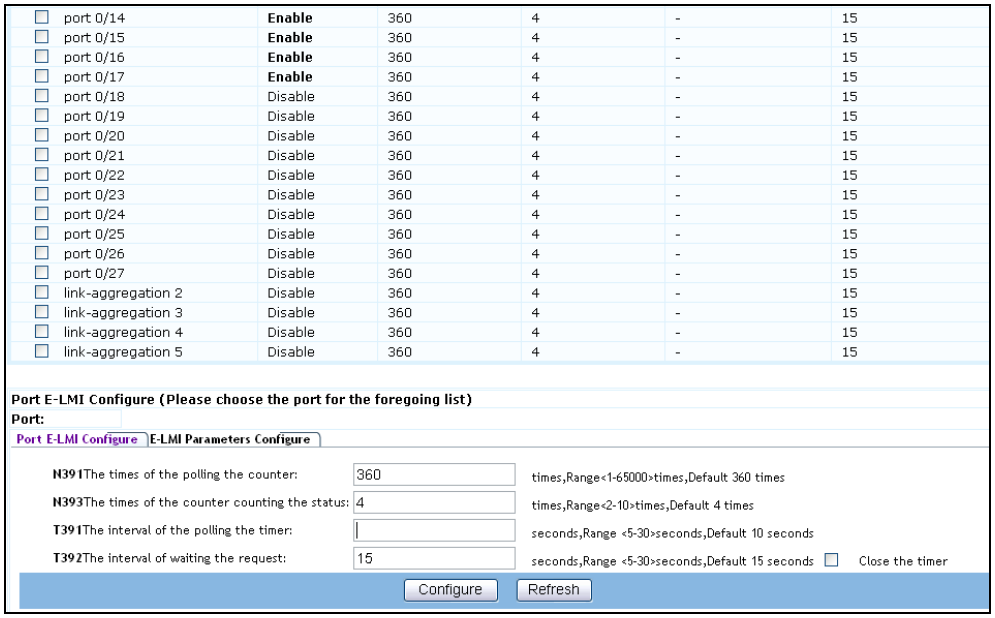
Enable the E-LMI function of the selected ports.

E-LMI Running Parameters on PE

Select the desired port, and click

.





In PE mode, T391 is invalid, so it is displayed “-“.

E-LMI Protocol Configuration on CE

Refer to the above section.

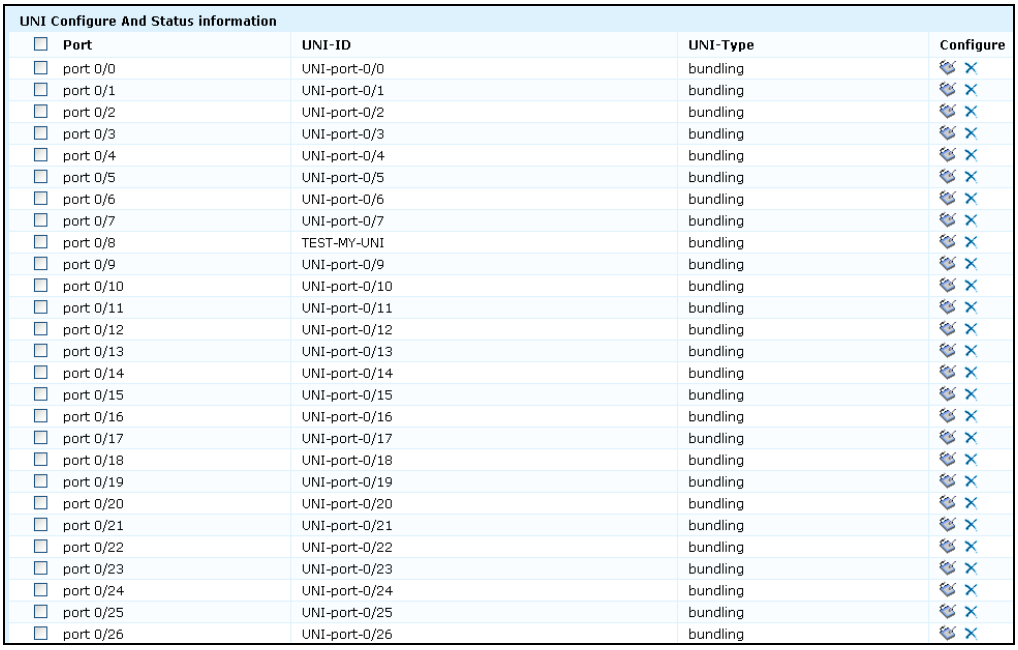
EVC-UNI Configuration

Configure the UNI type of the local port. Currently, there are three types, including bundling, all-to-one, and multiplexing.

Bundling: One UNI port can be bound to several EVCs, and one or several CEVLANs are mapped to the EVCs;

all-to-one: One UNI port is bound to only one EVC and all CEVLANs are mapped to the EVC;

multiplexing: One UNI port can be bound to several EVCs and only one CEVLAN is mapped to the EVCs.



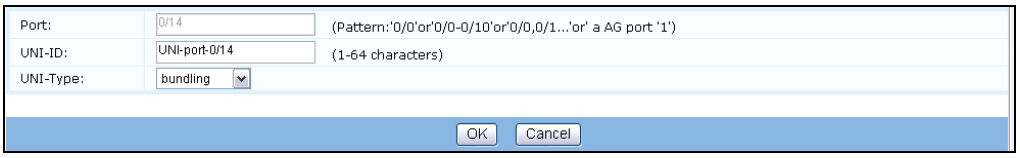
UNI Configure And Status information

Port	UNI-ID	UNI-Type	Configure
port 0/0	UNI-port-0/0	bundling	
port 0/1	UNI-port-0/1	bundling	
port 0/2	UNI-port-0/2	bundling	
port 0/3	UNI-port-0/3	bundling	
port 0/4	UNI-port-0/4	bundling	
port 0/5	UNI-port-0/5	bundling	
port 0/6	UNI-port-0/6	bundling	
port 0/7	UNI-port-0/7	bundling	
port 0/8	TEST-MY-UNI	bundling	
port 0/9	UNI-port-0/9	bundling	
port 0/10	UNI-port-0/10	bundling	
port 0/11	UNI-port-0/11	bundling	
port 0/12	UNI-port-0/12	bundling	
port 0/13	UNI-port-0/13	bundling	
port 0/14	UNI-port-0/14	bundling	
port 0/15	UNI-port-0/15	bundling	
port 0/16	UNI-port-0/16	bundling	
port 0/17	UNI-port-0/17	bundling	
port 0/18	UNI-port-0/18	bundling	
port 0/19	UNI-port-0/19	bundling	
port 0/20	UNI-port-0/20	bundling	
port 0/21	UNI-port-0/21	bundling	
port 0/22	UNI-port-0/22	bundling	
port 0/23	UNI-port-0/23	bundling	
port 0/24	UNI-port-0/24	bundling	
port 0/25	UNI-port-0/25	bundling	
port 0/26	UNI-port-0/26	bundling	

Only the ports on which the E-LMI protocol is enabled in PE mode can be displayed.

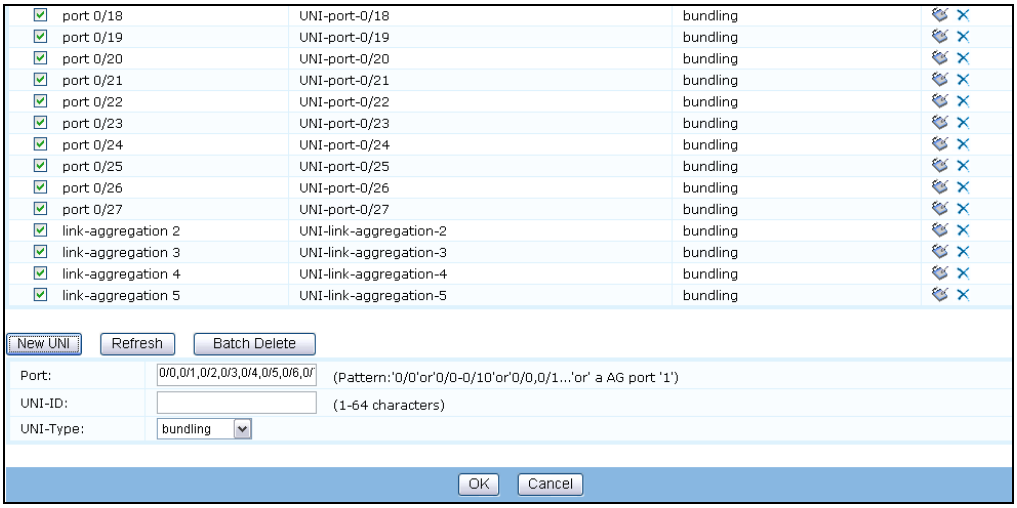
Edit

Click to edit the UNI-ID and UNI type of the port.



There is port and parameters. Here, port cannot be modified.

Batch edit: Select the desired port, and then click to edit the UNI-ID and the type of the port.

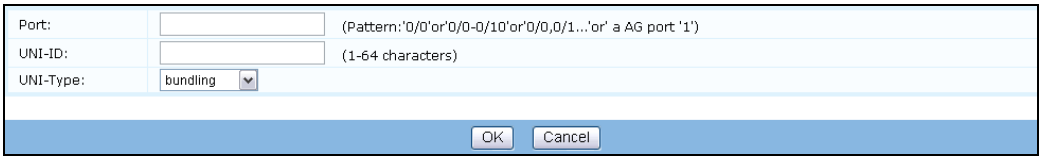


The default type is bundling.

Create New UNI

Click

, and then input the port.



Delete

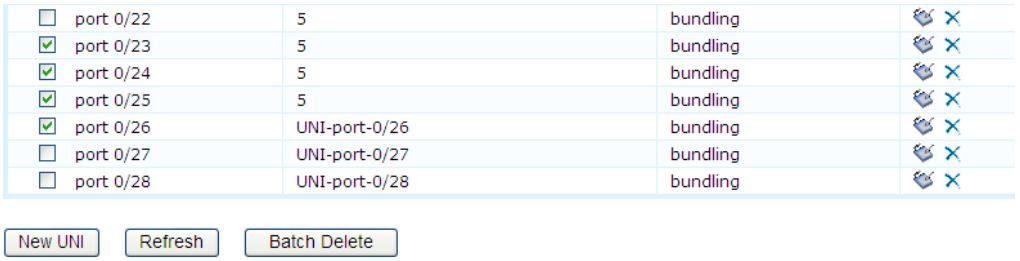
Delete Single

Click to delete the UNI-ID of the port and recover the system default value UNI-port-X/XX.

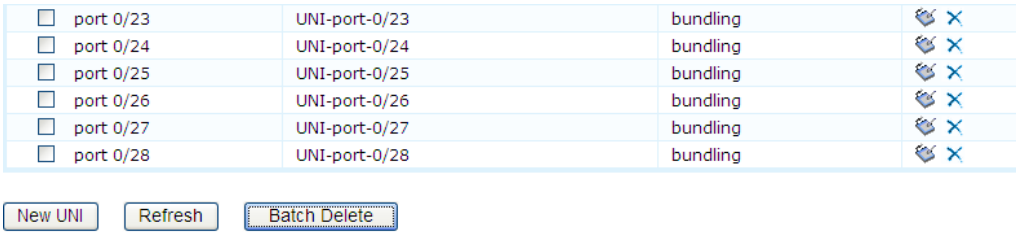
Batch Delete

Click

to delete the UNI-IDs of the selected ports and recover the system default value UNI-port-X/XX.



The result is as follows:



EVC Information

EVC is put forward by MEF. It is the virtual connection to connect two or more UNIs and switch Ethernet service frames between them. EVC can be divided to three types according to the connection mode.

- Point-to-point EVC (called Eline Service), including two types:

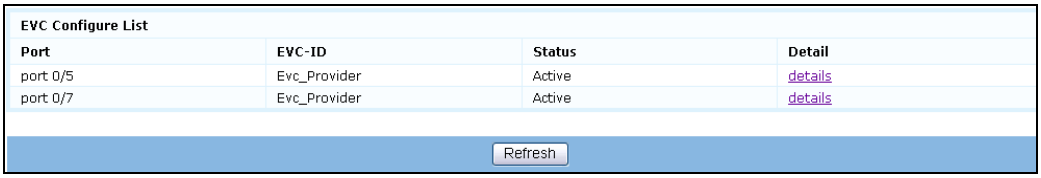
EPL: Ethernet provate line

EVPL: Ethernet virtual private line

The difference is that there can be several EVPLs on one UNI, while there can be only one EPL on one UNI. Currently, for RL08 QinQ, there is no difference and they both adopt one technology to realize. There is some difference only on the configuration.

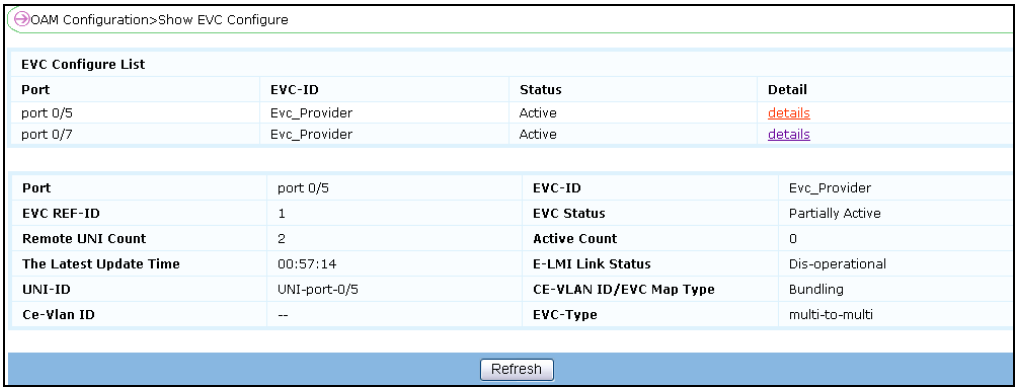
- Multipoint-to-multipoint EVC (called ELAN Service)

- Point-to-multipoint EVC: It is one special EVC. One end is called root and the other end is called leaf. The EVC comprises one or more roots (usually, it is one) + one or more leaves. The frames from the root node to the leaf node need to be copied to all leaves, while the frames from the leaf node to the root node only need to be transmitted to the root node. The frames are not copied between the leaf nodes. It is mainly used in IPTV. The RL08 device does not support the EVC directly, but it can support indirectly by configuring the port isolation and L3 forwarding between UNIs.



View Details

Click details to view the details.



Anti-Attack Detection Configuration

Overview

The chapter describes the configurations of the attack detection and scan detection.

Pseudo-source Address

Pseudo-source address is always the most common method used by the attacker for session hijack and DOS attack. The detection for this kind of packets is with technology. The most common detection is to configure the access list at the receiving direction on the interface to perform the packet filtering, but the detection is limited. The firewall function is enhanced this time. Meanwhile, other detection mechanisms are added. The detection is not omnipotent and not all the packets are valid, which does not mean that all detected packets are invalid.

The detection is performed in the following aspects:

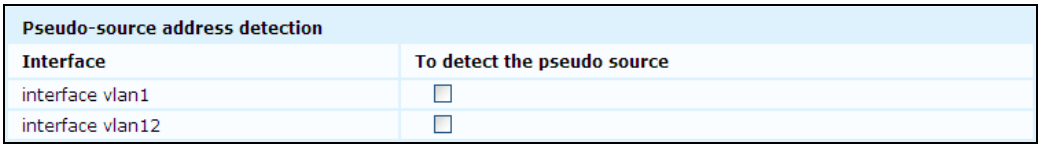
1. Whether the receiving port is correct: If the interface that receives one packet does not have the route to the source address, the route depends on the other interfaces, and the packet is held up (even it is not the deception of the pseudo-source address, it is at least abnormal);

2. The route to the source address of the packet cannot be found on the router and the packet is held up;

3. Seeing from the source address, it is the direct route (belonging to Ethernet) or interface router, but the corresponding items of the source MAC address and source IP address cannot be found in the ARP table, that is, the corresponding IP address of the MAC address is not consistent with the source IP address of the packet. It is likely to be deception. Hold up the packet.

4. Seeing from the source address, it is the gateway route, but the source address of the packet is the physical address of the gateway. It is likely to be deception. Hold up the packet.

5. The other packets: Release the normal or un-determined packets.



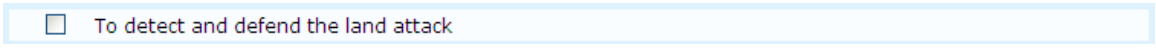
Attack Detection

LAND Attack Detection

Introduction to LAND

LAND attack uses another disadvantage of the system, that is, many systems do not how to deal with the problem that the SYN connection request whose source address and port number are equal to the destination address and port number results in the disorder or breakdown of the system. Therefore, if it is found that the source address of one packet is equal to the destination address and the source port number is equal to the destination port number, discard the packet.

ip tcp intercept land Configuration



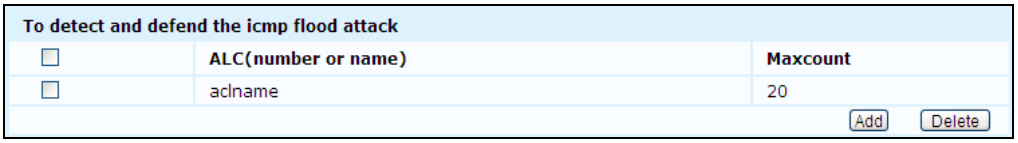
You only need to decide whether to enable the detection.

ICMP flood Attack Detection

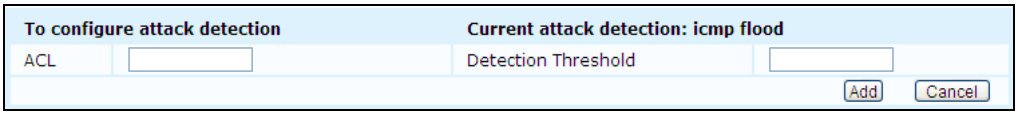
Introduction to ICMP flood

ICMP flood attack occupies the bandwidth by sending lots of ICMP packets to the target IP so that the valid packets cannot reach the destination, reaching the purpose of attack. During detection, record the ICMP packets whose destination addresses are L3 interface addresses of the switch. Once the receiving frequency of packets is higher than the normal range, it is doubted that there is attack and the flow frequency of packets is controlled strictly until the frequency is lower than the normal range. The processing method has some limitation, that is, the valid packets are also denied when denying the excessive packets. However, considering the bearing capability of the system, the method is the most reasonable.

ip icmp intercept Configuration



Click Add to configure new ICMP flood attack detection. Select the desired ICMP flood attack detection configurations, and click Delete to delete them.



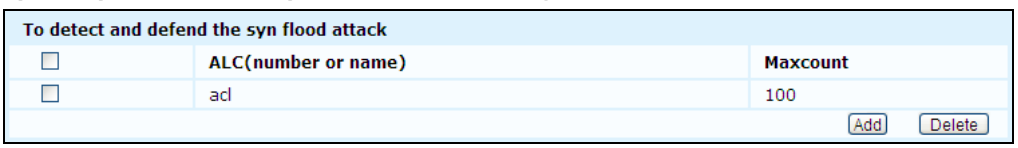
ACL: The ACL can be serial No., a number between 1 and 1000. It can also be the name of the ACL and only the standard ACLs are supported (the same below).

SYN flood Attack Detection

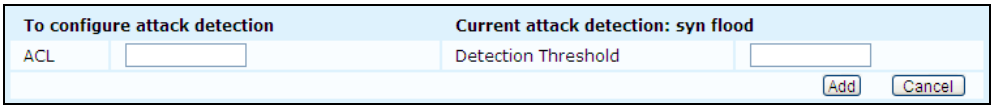
Introduction to SYN flood

SYN flood is the most famous attack for consuming the limited resources of the system. It is an attack of deliberate three-way handshake invasion and opening a large number of half-open TCP / IP connections. The attack adopts the IP deception to send the SYN request that seems to be valid to the attacked system. But in fact, the source address does not exist or is not online at the moment. Therefore, the response ACK message cannot reach the destination, while the attacked system is full of the half-open connections and the resources are consumed up. The valid connections cannot be responded. For the attack, you can use a simple holdup mode, that is, threshold holdup. Once the packet frequency of the SYN request received by one server exceeds the threshold, hold up the excessive. On one hand, the SYN attack intensity is reduced; on the other hand, it does not consume too many router resources and result in itself denying services. Note that the validity of the SYN packet is not distinguished, so it also results in the holdup of some valid requests. You can combine the pseudo-source address detection function to filter most attack packets, reducing the number of the valid packets that are held up.

ip tcp intercept list Configuration



Click Add to configure new syn flood attack detection; select the desired syn flood attack detection configuration and click Delete to delete it.

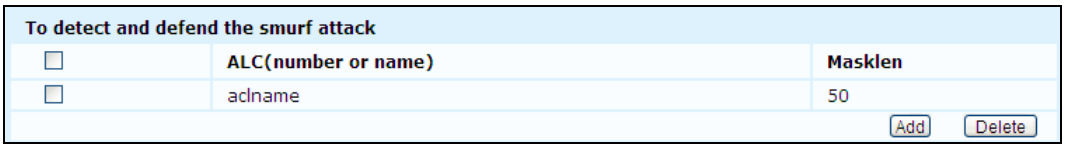


Smurf Attack Detection

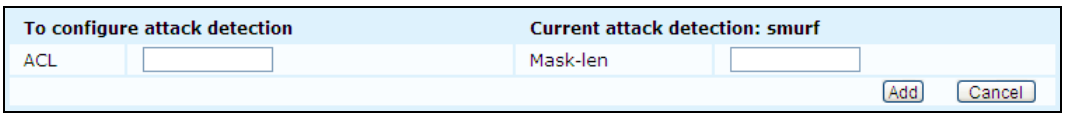
Introduction to Smurf

Smurf is also a kind of attack. The attacker first uses the address of the attacked host to send ICMP response request to one broadcast address; hundreds of PCs on the broadcast network make response; lots of response packets are sent to the attacked host. The result of the attack is the same as that of ICMP flood and more secret. This kind of packets can be held up by two methods. If pseudo-source address detection can find the packets, deny them directly. Besides, enable the smurf detection switch. If the source address is the address of the protected destination server, while the destination address is one broadcast address, hold up the packet. The smurf attack adopts the ICMP_ECHO packet, but considering that the other ICMP request packets can also lead to the same consequence, the detection is extended to ICMP_TSTAMP, ICMP_IREQ, and ICMP_MASKREQ packets.

ip smurf intercept Configuration



Click Add to configure new smurf attack detection. Select the desired smurf attack detection configuration and click Delete to delete it.



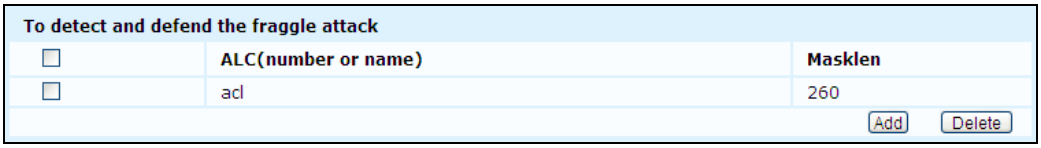
Fraggle Attack Detection

Introduction to Fraggle

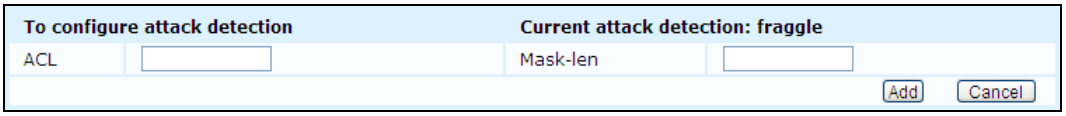
Strictly speaking, fraggle attack is the variant of smurf. When there are many firewalls to detect the ICMP packets strictly, fraggle does not send ICMP request packet to the broadcast address any more, but sends UDP

packets. When the PC of the destination segment receives the packet and finds that the destination port is unavailable, it sends one error packet of “the destination port is unavailable” to the attacked host. Lots of error packets rush into the attacked host at the same time, reaching the purpose of attacking the host. The fraggle attack detection is similar to smurf.

ip fraggle intercept Configuration



Click Add to configure new fraggle attack detection. Select the desired fraggle attack detection configuration and click Delete to delete it.

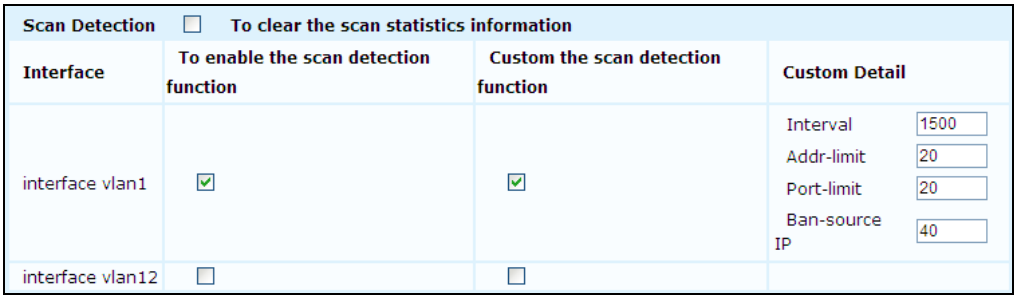


Scan Detection

Introduction to Scan Detection

The scan detection module can find the address scan and port scan attacks. By default, the system has a set of scan detection thresholds. The user can customize the scan threshold to reach the more detailed scan detection. When it is found that the scan happens to one address, the user can define prohibiting the access in a small period of time. The default value is 15s. Meanwhile, the system records the IP scan in the log for the user to analyze.

Scan Detection Configuration



Note

After the scan detection configuration is complete, click Configure to save the configuration.

Static Route Configuration

Overview

The chapter describes the static route configuration.

Introduction to Static Route

The static route is the customized route and is configured by the user manually. It makes the transmission of the IP packet between the source and destination adopt the specified path.

Compared with the dynamic routing protocol, the advantages of the static route include the security and the resource efficiency. The static route does not need to occupy the line bandwidth like the dynamic routing protocol. It can improve the network performance and does not need to occupy the CPU period to calculate and notify the route. The disadvantage is that when the network topology changes, it does not have the auto re-configuration mechanism and needs the user to configure manually.

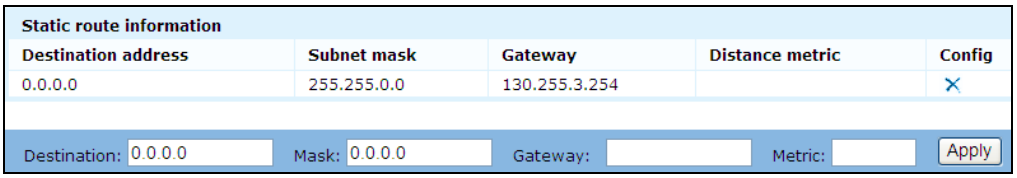
The static route can be re-distributed to the dynamic routing protocol, but the route of the dynamic routing protocol cannot be re-distributed to the static route table. Besides, the route loop caused by configuring the static route cannot be avoided.

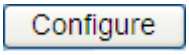
The static route is useful for the security of the small network. For example, there is only one path connected to the outer network. For the large-scale network, the static route can perform the security control for some services or links. Most networks adopt the dynamic routing protocol between the network devices, but one or two static routes can be configured for some special cases.

Configure Static Route

Configuring static route includes:

- Set the adding/deleting of static route;
- Set the management distance of static route;



Click  to add the configurations items of the static route.

DNS Configuration

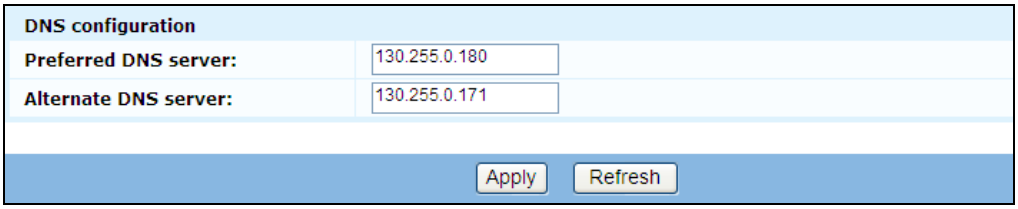
Overview

This chapter describes the DNS configuration.

DNS Server Configuration

IP defines one naming method, allowing one device to be identified by its location in IP. It is one hierarchical naming method for the domain. To keep the tacking of the domain name, IP defines the name server, which keeps the buffer (or database) of mapping the domain name to the IP address. To map the domain name to IP address, you first need to identify the host name and then specify the domain name server to make the domain naming system take effect. This is the global naming scheme of the Internet identifying the network device.

The **Preferred DNS server** and **Alternate DNS server** can be configured.



System Management

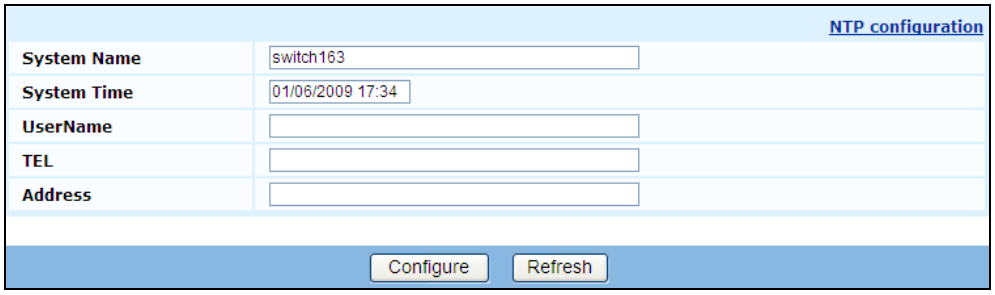
Overview

This chapter describes the system management configuration.

Basic Information Configuration

In Maipu switch, the main tasks of the system configuration are:

- Configure system name
- Configure system time



NTP Configuration

Click NTP configuration to enter the NTP configuration interface.

NTP Client Configuration

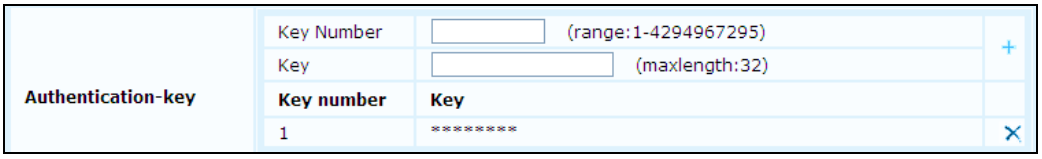
For the NTP client, the following items can be configured:

- Authentication-key
- Authenticate
- NTP Server

- Trusted-key

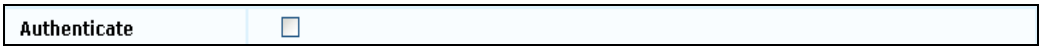
Besides, the Master configured on the server is cleared.

Authentication-key Configuration



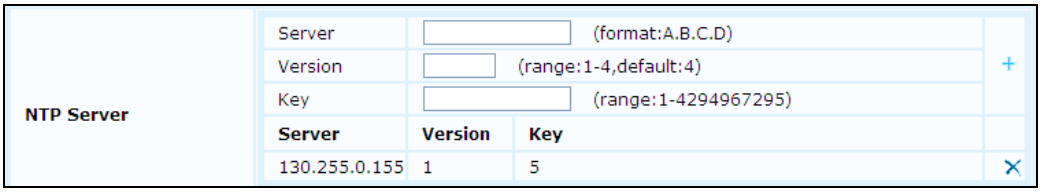
Click + to add configuration; click ✕ to delete the configuration.

Authenticate Configuration



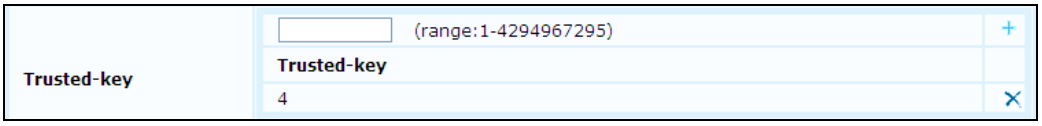
You only need to tick the check box.

NTP Server Configuration



Click + to add configuration; click ✕ to delete the configuration.

Trusted-key Configuration



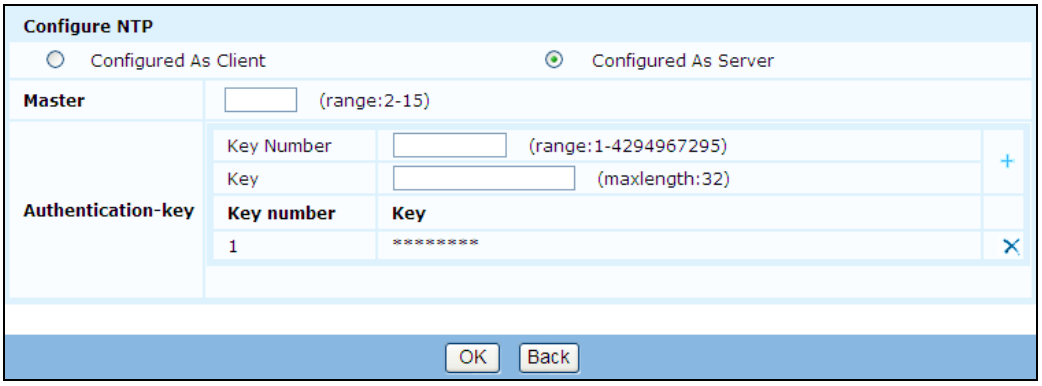
Click + to add configuration; click ✕ to delete the configuration.

NTP Server Configuration

For the NTP server, the following items can be configured:

- Master
- Authentication-key

Master Configuration



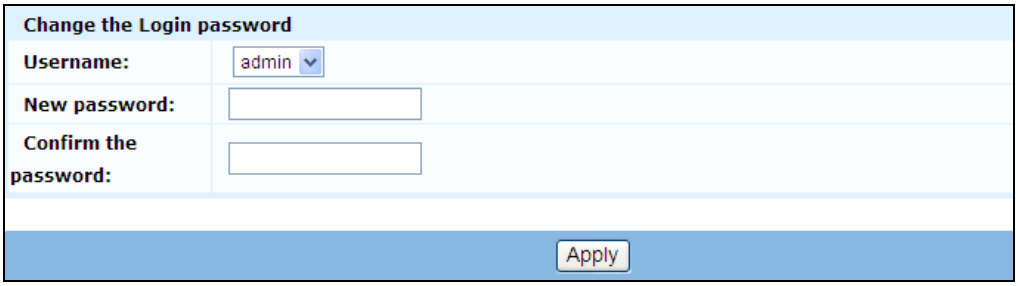
Authentication-key Configuration.

The same as **Authentication-key Configuration** in the section *NTP Client Configuration*

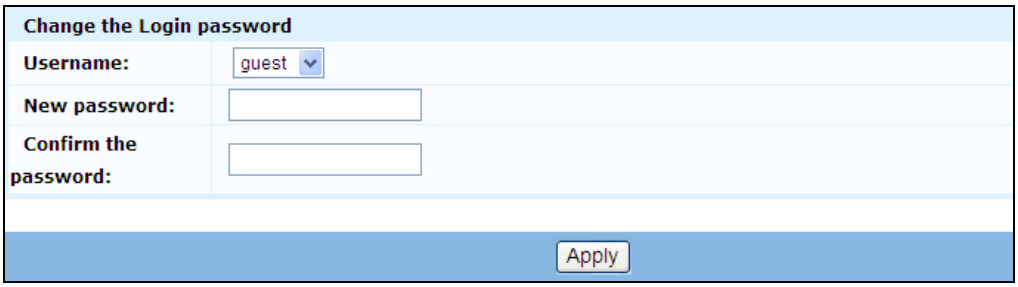
Administrator Configuration

Set the passwords of administrator and guest, set the password for entering the enable mode, set whether to enable guest user, and so on.

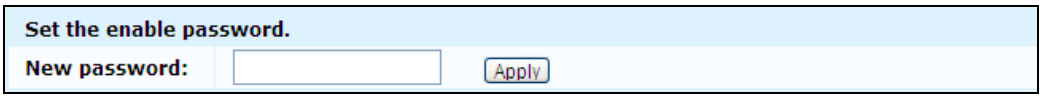
Set the password of the administrator as follows:



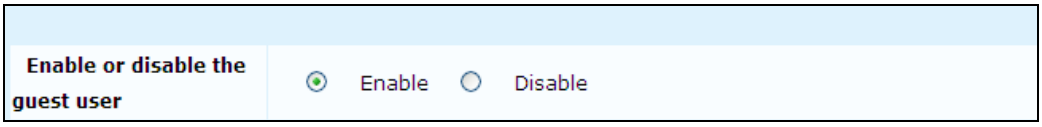
Set the password of the guest as follows:



Set the password for entering the enable mode as follows:



Set whether to enable the guest user as follows:



Device Software Upgrade

The system can select two kinds of file upgrade.

WEB file (*.rom)

ISO file (*.bin)

Click **Browse** to select the desired upgrade file.

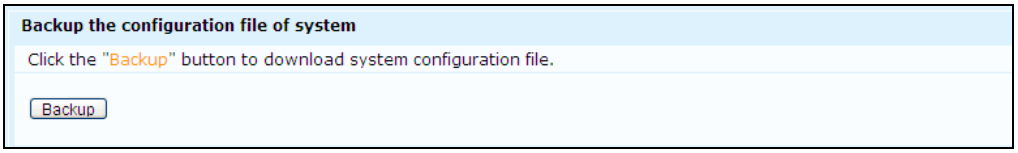
📖 Note

Re-start the device. The IOS program upgrade can take effect only after restarting the device.

Configuration File Management

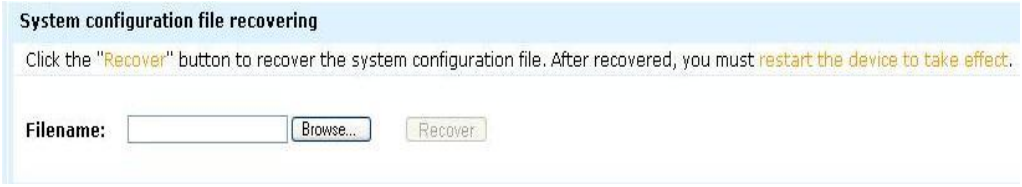
File management configuration includes:

The backup of the configuration files in the system:



Click **Backup** to back up the configuration files of the device to the local.

The recovering of the configuration files in the system:

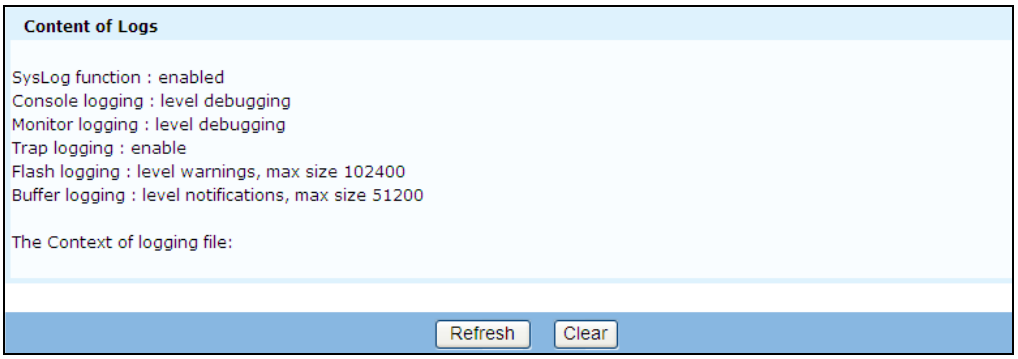


To recover to the previous configuration, find the desired configuration file at the local and click **Recover**.

Log Management

The system log function includes two aspects:

- Add some header information to the printed log message, such as time stamp and task name;
- Output and save the log message in various forms, including printing to the console port, printing to the telnet terminal via the switch, writing to the memory, writing to the flash file, sending to the log server and so on;



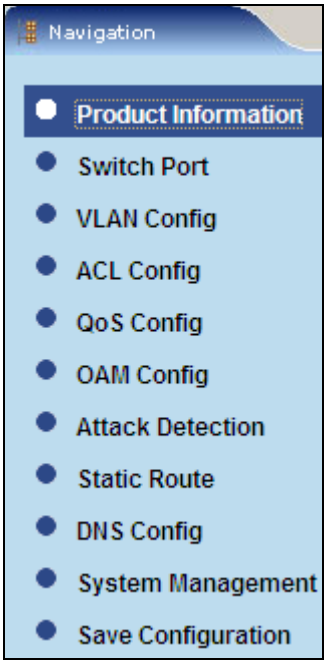
You can click Refresh to update the log information; click Clear to clear the current log information.

Save Configuration

Overview

The save function is to save all current configurations to the device.

After modifying the system configuration, the user can save the current configuration as the configuration parameters for enabling the switch next time



Click Save Configuration in the navigation and the system prompts a dialog box. Click **OK** to save the configuration or **Cancel** to cancel the saving operation.