GFS

S5800 Series Switches Web Management Guide

Models: S5800-8TF12S; S5800-48T4S; S5800-48F4SR; S5800-48MBQ



Contents

1. Web Login Configuration	1
1.1 HTTP Configuration	1
1.1.1 Management IP/ Route Configuration	1
1.1.2 User Configuration	
1.1.3 HTTP Configuration	
1.1.4 HTTPS Configuration	
1.1.5 Web Login	1
1.2 Introduction of Web Interface	2
1.2.1 Top Control Bar	4
1.2.2 Navigation Bar	5
1.2.3 Configuration Display Area	б
1.2.4 Bottom Area	б
1.2.5 Configuration Area	7
1.3 Device Summary	7
1.3.1 Interface Panel	7
1.3.2 Device Information	8
1.3.3 Device Monitor	9
2. Ethernet Status Configuration	10
2.1 Ethernet Status	
2.1.1 Basic Information	10
2.1.2 Interface Attribute Configuration	
2.2 Ethernet Stats	12
2.2.1 Basic Information	12
3. Link Aggregation Configuration	
3.1 Basic Information	16
3.1.1 Basic Information(S5800-8TF12S)	
3.2 Link Aggregation Global Configuration	
3.2.1 Global Configuration(S5800-8TF12S)	18
3.3 Link Aggregation Configuration	
3.3.1 User Configuration Add Link Aggregation	
3.3.2 User Configuration Edit Link Aggregation	22
3.3.3 Delete A Link Aggregation	
4. Storm Control	25
4.1 Storm Control	25
4.1.1 Basic Information	25
4.1.2 Storm Control Attribute Configuration	25
4.1.3 Unknown Unicast Storm Control	
4.1.4 Broadcast Storm Control	
4.1.5 Multicast Storm Control	
5. Flow Control	
5.1 Flow Control Display	29
5.2 Edit Flow Control	
6. Port Isolate	
6. Port Isolate	
6.1 Global Configuration	

-11-

6.2 Port Isolate Configuration	32
6.2.1 Port Isolate Group Information	32
6.2.2 Join the Port Isolation Group	33
6.2.3 Remove the Port Isolation Group	34
6.2.4 Modify the Port Isolation Group	35
6.2.5 Refresh the Port Isolation Group	37
7. Port Detect	38
7.1 Parameter Configuration	38
7.1.1 Basic Information	
7.1.2 Modify Parameter Configuration	39
7.2 Detect Configuration	40
7.2.1 Modify Error Recovery Function	41
8. VLAN	42
8.1 VLAN	42
8.1.1 Basic Information	42
8.1.2 Add or Delete VLAN	43
8.1.3 Modify VLAN	44
8.2 VLAN Interface	46
8.2.1 VLAN Interface Information	46
8.2.2 Add VLAN IF	46
8.2.3 Delete VLAN IF	
8.3 Acess/Trunk Port	48
8.3.1 Acess /Trunk Port Basic Information	
8.3.2 Access/Trunk Port Modification	
9. VLAN Classifier	52
9.1 VLAN Classifier Rules	52
9.1.1 Add VLAN Classifier Rules	52
9.1.2 Delete VLAN Classifier Rules	54
9.2 VLAN Classifier Groups	55
9.2.1 Add VLAN Classifier Groups	55
9.2.2 Delete VLAN Classifier Groups	56
9.3 VLAN Classifier Usage	57
9.3.1 Add VLAN Classifier Usage	57
9.3.2 Delete VLAN Classifier Usage	58
10. MAC	60
10.1 MAC Address Table	60
10.2 MAC Aging Time	61
10.3 MAC Learning	62
	63
10.4 Static MAC Table	
10.4 Static MAC Table	65
10.4 Static MAC Table 10.5 Blackhole MAC Table 10.6 Port Security	65 67
10.4 Static MAC Table 10.5 Blackhole MAC Table 10.6 Port Security 10.7 Static Security MAC	65 67 68
10.4 Static MAC Table	65 67 68 71
10.4 Static MAC Table 10.5 Blackhole MAC Table 10.6 Port Security 10.7 Static Security MAC 11. Spanning Tree 11.1 STP Information	65 67 68 71 71
10.4 Static MAC Table	
10.4 Static MAC Table	
10.4 Static MAC Table	

12. ERPS	81
12.1 ERPS Configuration	
12.1.1 Configure ERPS Mode	81
12.1.2 Add the ERPS Domain	
12.1.3 Add the ERPS Ring	
12.1.4 Modify the ERPS Ring	
12.1.5 Remove the ERPS Ring	
12.1.6 Modify the ERPS Domain	
12.1.7 Remove the ERPS Domain	
12.1.8 Refresh the ERPS Domain	
12.2 ERPS Status	92
12.2.1 ERPS Status Information	92
13. Mirror	
13.1 Mirror Configuration	94
13.1.1 Add Mirror Sessions	
13.1.2 Modify Mirror	97
13.1.3 Delete Mirror	
13.2 Global Configuration	
13.2.1 Configure Destination Port Forwarding Function	
13.3 Escape MAC for Remote Mirror	100
13.3.1 Add Escape MAC for Remote Mirror	101
13.3.2 Delete Escape MAC for Remote Mirror	
14. Multicast	
14.1 IGMP Snooping	
14.1.1 IGMP Snooping Global Configuration	
14.1.2 IGMP Snooping VLAN Configuration	
14.1.3 IGMP Snooping Information	
15. QOS	
15.1 Global Configuration	
15.1.1 Current QOS Status	
15.2 Interface Configuration	
15.2.1 Interface Configuration View	
15.2.2 Interface Attribute Configuration	
15.3 Port Policer	
15.3.1 Port Policer View	
15.3.2 Modify Port Policer	
15.4 Traffic Shaping	119
15.4.1 Traffic Shaping View	
15.4.2 Modify Traffic Shaping	
15.5 Congestion Manage	
15.5.1 Congestion Manage View	
15.5.2 Modify Congestion Manage	
15.6 Port Rate Limit	
15.6.1 Port Rate Limit View	
15.6.2 Modify Port Rate Limit	
16. ACL	127
16.1 Access Control List	

-IV-

16.1.1 ACL Configuration	
16.1.2 ACL Rules	
16.2 Class Map	134
16.2.1 Class map	134
16.2.2 Class Map Match ACL	
16.3 Policy Map	
16.3.1 Policy Map	139
16.3.2 Policy Map Match Class Map	
16.3.3 Policy Map Apply Interface	143
17. Reboot/Save	147
17.1 Page Overview	147
17.2 Save Configuration	
17.3 Reboot Switch	147
17.4 Recovery Switch	
18. System Configuration	
18.1 Base Settings	149
18.2 Thermal Sensor	
18.3 Base Information	
18.4 Date&Time	151
18.5 Time Zone Name	151
19. Load Configuration	153
19.1 Load Configuration	
- 19.1.1 Load the Configuration Files	
19.1.2 Refresh the Load Configuration Page	
19.1.3 Download the Configuration Files	
20. File Management	155
20.1 Memory Usage	
20.2 File Management	155
21. Log Management	159
21.1 Search Log Management	159
21.1.1 Search Log Information by Level	159
21.1.2 Search Log Information by Module	
21.2 Refresh Log Information	160
21.3 Clear Log Information	161
22. SNMP Configuration	
22.1 SNMP Basic Configuration	162
22.1.1 Enable SNMP	162
22.2 SNMP Group Configuration	
22.2.1 Add SNMP Group	163
22.2.2 Delete SNMP Group	163
23. SNMP Trap Configuration	
23.1 SNMP Trap Basic Configuration	
23.1.1 Enable SNMP Trap	
23.2 Trap Server Configuration	
23.2.1 Create Target SNMP Trap Server	
23.2.2 Delete SNMP Trap Server	

24. Worm Intercept	167
24.1 Worm intercept Configuration	
24.1.1 Current Worm Intercept Information	
24.1.2 Add Worm Intercept Rule	
24.1.3 Delete Worm Intercept Information	169
24.1.4 Clear the Defense Attack Packet Statistics	
24.1.5 Refresh Worm Intercept Page	
25. DDoS Intercept	
25.1 DDoS Intercept Page	171
25.2 DDoS Intercept Setting	172
26. ARP Intercept	
27. Currently Sessions	174
27.1 Current Sessions Information	174
27.2 Delete Current Sessions	
28. User Management	176
28.1 Add User	
28.2 Edit User	
28.3 Delete User	
28.4 Refresh	
29. IP Routing	
29.1 IPv4 Route	
29.1.1 Current Routing Information	
29.2 IPv4 Static	
29.2.1 IPv4 Static Route Information	
29.2.2 Add IPv4 Static Route	
29.2.3 Delete IPv4 Static Route	
29.2.4 Modify IPv4 Static Route	
30. Ping	
31. Traceroute	
31.1 Traceroute	
31.2 Implement Tracert Ping Test	186
32. Virtual Cable Test	

1. Web Login Configuration

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through web browser, the switches support the HTTP configuration, the abnormal packet timeout configuration, and so on.

1.1.1 Management IP/ Route Configuration

Before web network management client can access switch by HTTP, user should configure the management IP and route by CLI on switch.

Command	Purpose
management ip address 10.10.38.2/23	Configure the management IP
management route add gateway 10.10.39.254	Configure the management route

1.1.2 User Configuration

User should add logging user by CLI before access switch by HTTP.

Command	Purpose			
username admin password admin	add logging username and password			

1.1.3 HTTP Configuration

Switches support to control the HTTP access, only when the HTTP service is enabled can HTTP exchange happen between switch and PC, when the HTTP service is closed, HTTP exchange stops, if you want to open HTTP service, please follow the following steps by CLI on switch:

- (1) Use tftp or ftp to copy web image to the flash:
- copy mgmt-if tftp://192.168.0.1/webImage.bin flash:/webImage.bin
- (2) Load web image:
- http server load flash:/webImage.bin
- (3) Enable HTTP service for web network management : service http enable

1.1.4 HTTPS Configuration

In order to improve the security of communications, switches support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

Command	Purpose
service https enable	Enable HTTPS service for web network management

1.1.5 Web Login

After configuration by CLI on switch, you can follow the following steps to login web page:

- (1) Open IE browser, input address field with URL (universal resource locator) address of the switch.
- (2) Enter username and password which user created with CLI(default is admin/admin), the login page is shown as the figure 1.
- (3) Enter the main page.



Figure 1 Web login page

1.2 Introduction of Web Interface

The web network management divided four categories: Monitor, Configuration, Maintenance, Network.
The structure of the monitor page is slightly different from that of the other three pages.
(1) Monitor

The Web monitor page appears after login, as shown in figure 2.

FS S5800-8TF1	25		Monitor	Configuration	X Maintenance	Network			Save	admin	
Monitor									Auto refresh Ma	nual 💌	🖒 Refresh
Interface Panel											
	STOC NO SS800-8TF125	14.¥2 34.¥4 54	× ¥6 7.4 ¥8	14 ¥2 34 ¥4 9 1111 1111 1111 1111 1111 1111 100/1000 BA	SA V 6 7A V 8 1111 1111 2.000 2.52 1111 1111 5E-X			18 A ¥ 14 15 A ¥ 16	17.4 ¥ 18 19.4 ¥ 20 1111 1111 ¥.4 ¥.4 ¥.4 ¥.4 1111 1111		
Device Information			💼 Electrica	I 🔲 Optical	Active Inactive	Disabled					
Product ID	S5800-8TF12S		Image Name	centecC	S-e350-8ts12x-v5.3.11.6.r.bin	0	Serial Numbe	er CG	1907065314N0027		
Location	wuhan		WebImage Nam	e flash:/35	50-6-18.bin		MAC Address	5 64	:9D:99:00:E4:B1		
Device Name	8TF12S-126		BootRom Versio	n 7.1.4			Uptime	1 c	days, 23 hours, 58 minutes		
Contact	fs.com		Hardware Versio	n 2.0			PWR 1	PR	ESENT ; OK ; AC		
Software	FSOS, 5.3.11.6		EPLD Version	1.2			PWR 2	PR	ESENT ; FAIL ; AC		
Usage			Tempe	rature			Fan				

Figure 2 Web monitor page

The whole monitor page consists of the top control bar, the configuration display area and the bottom area. (2) Configuration

If you click "Configuration" in the top control bar, as shown in figure 3.

FS [\$5800-8TF125]			Monitor	Configuration	X Maintenance	T Network		Save admin Logou
Ethernet Status	Ethernet Status	Ethernet Stats						
轉 Link Aggregation	Falterment Sheeters							
3 Storm Control	Ethernet status							
Flow Control	Refres	n						
🗎 Port Isolate	Interface Name	Status	Duplex	Speed(Mbit/s)	Mode	Туре	Description	Operation
Port Detect	🖾 eth-0-1	down	auto	auto	trunk	Unknown		Edit
님 VLAN	🔲 eth-0-2	up	a-full	a-1000	access	1000BASE_T		Edit
BB VLAN Classifier	🔲 eth-0-3	down	auto	auto	access	Unknown		Edit
MAC	🔲 eth-0-4	down	auto	auto	access	Unknown		Edit
😫 Spanning Tree	🔲 eth-0-5	down	auto	auto	access	Unknown		Edit
≪∂ ERPS	🔲 eth-0-6	down	auto	auto	access	Unknown		Edit
I Mirror	🔲 eth-0-7	down	auto	auto	access	Unknown		Edit
$\delta^{\underline{Q}}_{b}$ Multicast	🔲 eth-0-8	down	auto	auto	access	Unknown		Edit
🙉 QOS	🔲 eth-0-9	down	auto	auto	access	Unknown		Edit
🖄 ACL	🔲 eth-0-10	down	auto	auto	access	Unknown		Edit

Figure 3 Web configuration page

The whole configuration page consists of the top control bar, the navigation bar, the configuration area and the bottom area. (3) Maintenance

If you click "Maintenance" in the top control bar, as shown in figure 4.

FS 55800-8TF125		Monitor Con	Diguration Mai	K ntenance Ne	twork	Save admin Logout
Reboot/Save System Configuration Load Configuration File Management Log Management SNMP SNMP SNMP Worm Intercept DDoS Intercept	Save configuration to startup-config Save configuration to startup-config Reboot the switch Reboot the switch Restore factory configuration to startup-con Restore factory configuration to startup-con	Monitor Con Save Save Save Save Save Save Save Save	figuration Mai	Itenance N		
ARP Intercept Currently Sessions R User Management			Copyright © 2009-21	20 FS.COM Inc . All Right	b Reserved,	

Figure 4 Web maintenance page

The whole maintenance page consists of the top control bar, the navigation bar, the configuration area and the bottom area. (4) Network(4) If you click "Network" in the top control bar, as shown in figure 5.

FS [\$5800-8TF125]		Monitor	Configuration	X Maintenance	Network	Save admin Logout
IP Routing	IPv4 Routing Table Information	IPv4 Static Route Info	rmation			
Ding Ping						
P Traceroute	IPv4 Routing Table Information					
	Protocol			Query		
	Destination	Mask		Protocol	Nexthop	Outgoing Interface
	192.168.1.0	255.255.255.0(24)	Direct		vlan1
	192.168.1.119	255.255.255.25	5(32)	Direct		vlan1
	Total 2 records.					10 🔻 🔿
			Copyrigh	t © 2009-2020 FS.COM Inc	. All Rights Reserved.	

Figure 5 Web network page

The whole network page consists of the top control bar, the navigation bar, the configuration area and the bottom area.

1.2.1 Top Control Bar

GFS 55800-8TF125	Monitor	Configuration	X Maintenance	Network	Save admin Logout

Figure 6 Top control bar

• Parameter usage

ltem	Description			
Monitor	Display interface panel, basic information and monitor of the device			
Configuration	Including switch port common configuration and layer-2 protocol, etc			
Maintenance	Including switch system configuration and some security configuration, etc			
Network	Including IP route configuration, ping and trace route function			
Save	Click the Save button will jump to "Maintenance -> Reboot/Save", then click "save" button, write the current settings to the configuration file of the device, it is equivalent to the execution of the write command			
Username	Display the current web login user			
Logout After you click "logout", you have to enter the username and the password ag				

1.2.2 Navigation Bar



Figure 7 Navigation control bar

For example, to browse the flux of the current port, you have to click "Ethernet Status" and then "Interface State" configure.

FS 55800-8TF125			Monitor	Configuration	% Maintenance	Network		Save admi	n 🕴 Logout
Ethernet Status	Ethernet Status	Ethernet Stats		1					
M Link Aggregation	Ethorpot Ctatur								
🕱 Storm Control	Ethernet Status								
15 Flow Control	Edit	9							
Port Isolate	Interface Name	Status	Duplex	Speed(Mbit/s)	Mode	Туре	Description		Operation
Port Detect	🔲 eth-0-1	down	auto	auto	trunk	Unknown			Edit
님 VLAN	🔲 eth-0-2	up	a-full	a-1000	access	1000BASE_T			Edit
B VLAN Classifier	🔲 eth-0-3	down	auto	auto	access	Unknown			Edit
MAC	🔲 eth-0-4	down	auto	auto	access	Unknown			Edit
留 Spanning Tree	🔲 eth-0-5	down	auto	auto	access	Unknown			Edit
& ERPS	🔲 eth-0-6	down	auto	auto	access	Unknown			Edit
I Mirror	🔲 eth-0-7	down	auto	auto	access	Unknown			Edit
暑 Multicast	🔲 eth-0-8	down	auto	auto	access	Unknown			Edit
QOS	🔲 eth-0-9	down	auto	auto	access	Unknown			Edit
🖄 ACL	🔲 eth-0-10	down	auto	auto	access	Unknown			Edit
				Copyright	© 2009-2020 FS.CON	I Inc . All Rights Reserv	ved.		

Figure 8 Interface state configure

1.2.3 Configuration Display Area

The configuration display area shows the state and configuration of the device, as shown in figure 9.

Monitor					Auto refresh Manual 🔻 🔿 Refresh
Interface Panel					
	EX 80 € FS 51800 477125	Y4 54 Y4 74 Y4 14	YZ IA.YE IA.YE IA.YE TIT TIT TIT TIT STATE TIT TIT TIT		
		dh Elec	trical 🥅 Optical 📕 Active 🖬 Inactive 📕 Disabled		
Device Information					
Product ID	\$\$800-8TF125	Image Name	centecOS-e350-8ts12x-v5.3.11.6.r.bin	Serial Number	CG1908020298N0021
Location	**	WebImage Name	flash:/webimage-e350-5.3-en.bin	MAC Address	64:9D-99:00:E8:81
Device Name	\$5800-8TF12S-119	BootRom Version	7.1.4	Uptime	0 days, 0 hours, 30 minutes
Contact		Hardware Version	2.0	PWR 1	PRESENT ; FAIL ; AC
Software	PS05, 5.3.11.6	EPLD Version	12	PWR 2	PRESENT ; OK ; AC

Figure 9 Configuration display area

1.2.4 Bottom Area

The bottom area shows the company copyright information, as shown in figure 10.

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Figure 10 Bottom control bar

1.2.5 Configuration Area

Ethernet Status	Ethernet Stats						
Ethernet Status							
Edit Refre	rsh						
Interface Name	Status	Duplex	Speed(Mbit/s)	Mode	Туре	Description	Operation
🗌 eth-0-1	up	a-full	a-100	access	1000BASE_T		Edit
🗌 eth-0-2	down	auto	auto	access	Unknown		Edit
🗌 eth-0-3	down	auto	auto	access	Unknown		Edit
🗌 eth-0-4	up	a-full	a-1000	access	1000BASE_T		Edit
🗌 eth-0-5	up	a-full	a-1000	access	1000BASE_T		Edit
🗌 eth-0-6	down	auto	auto	access	Unknown		Edit
🗌 eth-0-7	down	auto	auto	access	Unknown		Edit
🗌 eth-0-8	down	auto	auto	access	Unknown		Edit
🗌 eth-0-9	down	auto	auto	access	Unknown		Edit
🗌 eth-0-10	down	auto	auto	access	Unknown		Edit

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved

Figure 11 Configuration area

The configuration area is to show the content that is selected in the navigation area, the configuration area always contains one or more buttons, and their functions are listed in the following table.

•	Parameter	usaq	e
	i ururreter	asag	-

ltem	Description
Refresh	Refresh the content shown in the current configuration area
Apply	Apply the modified configuration to the device, the application of the configuration does not mean that the configuration is saved in the configuration file, to save the configuration, you have to click " Save " on the top control bar
New	Creates a list item, for example, you can create a VLAN item or a new user
Network	Including IP route configuration, ping and trace route function
Delete	Deletes an item in the list
Back	Go back to the previous-level configuration page
Edit	Modified configuration to the device

1.3 Device Summary

If you click "Monitor" in the top control bar, the device summary page appears, as shown in figure 12.

F FS 55800-877125	Monitor	Configuration	* Maintenance	A Network	Save admin Logout
Monitor					Auto refresh Manual 🔻 🔿 Refresh
Interface Panel					



This chapter describes all components of logon homepage, including device panel, device information and device monitor.

1.3.1 Interface Panel

Click "Monitor" to check interface panel status on switch, the configuration page is shown as the figure 13.

		Auto refresh	Manual 🔻	3) Refresh
Interface Panel					
	13 • • 14 15 • • 16	17.4.¥18 19.4.¥ 20			

Figure 13 Interface panel

Based on type of the switch connected, the display area of web interface panel can intuitively display information of the various interfaces of this switch, the contents displayed including: Interface amount. Operating statuses of interfaces: including activated state and interface type.

• Parameter usage

ltem	Description
Auto refresh Refresh the page in specified time	

1.3.2 Device Information

Click "Monitor" to check device information status on switch, the configuration page is shown as the figure 14.

Device Information					
Product ID	\$5800-8TF125	Image Name	centecOS-e350-8ts12x-v5.3.11.6.r.bin	Serial Number	CG1908020298N0021
Location		WebImage Name	flash:/350-6-15.bin	MAC Address	64:9D:99:00:E8:B1
Device Name	\$5800-8TF12S-119	BootRom Version	7.1.4	Uptime	0 days, 1 hours, 0 minutes
Contact		Hardware Version	2.0	PWR 1	PRESENT ; FAIL ; AC
Software	FSOS, 5.3.11.6	EPLD Version	1.2	PWR 2	PRESENT ; OK ; AC

Figure 14 Device information panel

• Parameter usage

ltem	Description				
Product ID	The hardware product of the switch				
Location	Indicate the location of the switch				
Device Name	Indicate the host name of the switch				
Contact	Indicate the contact of the switch				
Software	The software version of the switch				
Image Name	The name of the boot image				
BootRom Version	Indicate the Boot Rom version of the switch				

ltem	Description					
Hardware Version	Indicate the hardware version of the switch					
EPLD Version	Indicate the EPLD version of the switch					
Serial Number	Indicate the serial number of the switch					
MAC Address	The system mac of the switch					
Uptime	Indicate the uptime of the switch					
PWR 1	Indicate the current status of power 1					
PWR 2	Indicate the current state of power 2					

1.3.3 Device Monitor

Click "Monitor" to check device monitor status on switch, the configuration page is shown as the figure 15.



Copyright © 2009-2020 FS.COM Inc. All Rights Reserved.

Figure 15 Device summary panel

Parameter usage

Item	Description					
CPU Usage	Indicate the CPU usage of the switch					
Memory Usage	Indicate the software memory usage of the switch					
Temperature	Indicate the current temperature of the switch					
FAN	Specify the fan number and ID					
Status	Indicate the current work status of each fan					
Speed Rate	Indicate the current work speed rate of the switch					

2. Ethernet Status Configuration

If you click "Configuration->Ethernet Status" in the top control bar, the ethernet status configuration list page appears, as shown in figure 1.

FS 55800-8TF125			Monitor	Configuration	% Maintenance	Th Network		Save adm	in Logout
Ethernet Status 2	Ethernet Status	Ethernet Stats							
00 Link Aggregation	54								
III Storm Control	Ethernet Status								
E Flow Control	Edit Refres	h							
Port Isolate	Interface Name	Status	Duplex	Speed(Mbit/s)	Mode	Туре	Description		Operation
Port Detect	🗌 eth-0-1	down	auto	auto	access	Unknown			Edit
님 VLAN	eth-0-2	down	auto	auto	access	Unknown			Edit
88 VLAN Classifier	🗋 eth-0-3	down	auto	auto	access	Unknown			Edit
MAC	eth-0-4	down	auto	auto	access	Unknown			Edit
🗄 Spanning Tree	🗋 eth-0-5	up	a-full	a-1000	access	1000BASE_T			Edit
d₀ ERPS	🗋 eth-0-6	down	auto	auto	access	Unknown			Edit
Mirror	🗌 eth-0-7	down	auto	auto	access	Unknown			Edit
${}^{\mathbb{Q}}_{\hat{\sigma}\hat{\sigma}}$ Multicast	eth-0-8	down	auto	auto	access	Unknown			Edit
🙉 qos	🗌 eth-0-9	down	auto	auto	access	Unknown			Edit
C ACL	🗌 eth-0-10	down	auto	auto	access	Unknown			Edit

Figure 1 Ethernet status configuration list

This chapter describes the interface configuration function of the switch.

2.1 Ethernet Status

This section mainly describes how to configure and view interface connection.

2.1.1 Basic Information

If you click "Ethernet Status -> Ethernet Status" to check each interface status on switch, the configuration page is shown as the figure 2.

Ethernet Status							
Edit Refrest	h						
Interface Name	Status	Duplex	Speed(Mbit/s)	Mode	Туре	Description	Operation
🗌 eth-0-1	down	auto	auto	access	Unknown		Edit
🗌 eth-0-2	down	auto	auto	access	Unknown		Edit
🗌 eth-0-3	down	auto	auto	access	Unknown		Edit
🗌 eth-0-4	down	auto	auto	access	Unknown		Edit
🗌 eth-0-5	up	a-full	a-1000	access	1000BASE_T		Edit
🗌 eth-0-6	down	auto	auto	access	Unknown		Edit
🗌 eth-0-7	down	auto	auto	access	Unknown		Edit
🗌 eth-0-8	down	auto	auto	access	Unknown		Edit
🗌 eth-0-9	down	auto	auto	access	Unknown		Edit
🗌 eth-0-10	down	auto	auto	access	Unknown		Edit

pyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Parameter usage

ltem	Description
Interface Name	Display the number of interface

Status	The operating status (up or down) on interface
Duplex	Display the current duplex configuration on the interface
Speed(M bit/s)	Display the current speed configuration on the interface
Mode	Display the switch port mode of interface
Туре	Display the media type of interface
Description	Description about the interface
Operation	Display that interface configuration properties can be edited

2.1.2 Interface Attribute Configuration

If you want to modify the configuration to interface attribute, you can follow the following steps:

- Please click "Edit" button or select a check box for one or more interfaces and click the "Edit" button. (1)
- Select "Up/Down" in the "Admin Status" radio box. (2)
- (3) Select "L2 mode/L3 mode" in the "L2/L3 Mode" radio box.
- Select "Trunk/Access" in the "Mode" radio box. (4)
- (5)
- Select "Enable/Disable" in the "Jumbo frame" radio box. Select speed configure in the "Speed" drop-down box. (6)
- Enter interface description in the "Description" text box. (7)
- (8) After that, click "Apply" to apply all the changes made.

Ethernet Statu	S						
1 Edit	Refresh						
Interface	e Name Status	Duplex	Speed(Mbit/s)	Mode	Туре	Description	Operation
🗹 eth-0-1	down	auto	auto	access	Unknown		1 Edit
🗌 eth-0-2	down	auto	auto	access	Unknown		Edit
🗌 eth-0-3	down	auto	auto	access	Unknown		Edit
🗌 eth-0-4	down	auto	auto	access	Unknown		Edit
🗌 eth-0-5	up	a-full	a-1000	access	1000BASE_T		Edit
🗌 eth-0-6	down	auto	auto	access	Unknown		Edit
🗌 eth-0-7	down	auto	auto	access	Unknown		Edit
🗌 eth-0-8	down	auto	auto	access	Unknown		Edit
🗌 eth-0-9	down	auto	auto	access	Unknown		Edit
🗌 eth-0-10) down	auto	auto	access	Unknown		Edit

Copyright © 2009-2020 FS.COM Inc . All Rights Rese

Figure 3 Interface status operation

terface Management						
Interface Name	eth-0-1					
Interface Current Status	Down					
* Admin Status	🖲 Up	🔵 Down	2			
* L2/L3 Mode	L2 mode	🔿 L3 mode	3			
* Mode	🔿 Trunk	Access	4			
* Jumboframe	🔵 Enable	Disable	5			
* Speed	Auto	○ 10M	○ 100M	◯ 1000M	<u> 0 10</u> G 6	
Description	Please ent	ter description				
				(Less than 256 c	haracters)	7
	8 Apply	Back				

Figure 4 Interface attribute configuration

• Parameter usage

ltem	Description						
Interface Name	Display the number of interface						
Interface Current Status	The Current status (up or down) on interface						
Admin Status	The operating status (up or down) on interface						
L2/L3 Mode	Display the L2/L3 mode of interface						
Mode	Display the switch port mode of interface						
Jumboframe	Specific set of machines that you manage and configure						
Speed(M bit/s)	Display the current speed configuration on the interface						
Description	Description about the interface						

2.2 Ethernet Stats

This section mainly describes how to show interface stats.

2.2.1 Basic Information

If you click "Ethernet Status -> Ethernet Stats" to view statistics information for each interface, statistics on interface is accounted after device start up completed, show as the figure 5.

FS 5800-8TF125		Monitor	Configuration	X Maintenance	Network	Save admin Logout
🖱 Ethernet Status 1	Ethernet Status	thernet Stats 2				
00 Link Aggregation						
🐹 Storm Control	Ethernet Stats					
Flow Control	Clear Stats Refr	resh				
Port Isolate	Interface Name	Output Packets	Output Bytes	Input Packets	Input Bytes	Operation
Port Detect	eth-0-1	0	0	0	0	Edit
님 VLAN	eth-0-2	0	0	0	0	Edit
88 VLAN Classifier	eth-0-3	0	0	0	0	Edit
MAC	eth-0-4	0	0	0	0	Edit
留 Spanning Tree	eth-0-5	0	0	0	0	Edit
48 ERPS	eth-0-6	0	0	0	0	Edit
Mirror	eth-0-7	0	0	0	0	Edit
$\mathcal{J}_{6}^{\overline{\mu}}$ Multicast	eth-0-8	0	0	0	0	Edit
a qos	eth-0-9	0	0	0	0	Edit
🖄 ACL	eth-0-10	0	0	0	0	Edit

Figure 5 Ethernet stats page

Interface Name	Output Packets	Output Bytes	Input Packets	Input Bytes
eth-0-1	0	0	0	0
eth-0-2	0	0	0	0
eth-0-3	0	0	0	0
eth-0-4	0	0	0	0
eth-0-5	0	0	0	0
eth-0-6	0	0	0	0
eth-0-7	0	0	0	0
eth-0-8	0	0	0	0
eth-0-9	0	0	0	0
eth-0-10	0	0	0	0
eth-0-11	1795	658765	0	0
eth-0-12	0	0	0	0

Copyright © 2019 by FS.COM All Rights Reserved.

Figure 6 Statistics on interface

If you want to clear the ethernet stats, please click "Clear Stats" button, shown as the figure 7. Ethernet Stats Ethernet Stats

Ethernet Stats Refresh Clear Stats Interface Name Output Packets Out Operation put Bytes tips × eth-0-1 0 0 Edit eth-0-2 0 0 Edit Are you sure to Clear Statistics? 0 eth-0-3 0 Edit eth-0-4 0 0 Edit Cancel eth-0-5 0 0 Edit eth-0-6 0 0 Edit 0 0 0 0 eth-0-7 0 Edit eth-0-8 0 0 Edit 0 0

14

Figure 7 Interface detail clear stats

Choose one interface to enter the interface statistics detail page, shown as the figure 8.

Interface Name:eth-0-4	
Item	Statistics
Received Statistics	
Packets Input	0
Bytes Input	0
5 Minute Input Rate(packets/sec)	0
5 Minute Input Rate (bits/sec)	0
Unicast Packet	0
Broadcast Packet	0
Multicast Packet	0
Runts	0
Giants	0
Input Errors	0
CRC	0
Frame	0
Pause	0
Sent Statistics	
Packets Output	0
Bytes Output	0
5 Minute Output Rate(packets/sec)	0
5 Minute Output Rate (bits/sec)	0
Unicast Packet	0
Broadcast Packet	0
Multicast Packet	0
Output Errors	0
Pause	0

Figure 8 Detail statistics on interface

15

• Parameter usage

ltem	Description				
Interface Name	Display the number of interface				
Output Packets	Total packets sent on this interface				
Output Bytes	Total bytes including frame characters sent on this interface				
Input Packets	Total packets received on this interface				
Input Bytes	Total bytes including frame characters received on this interface				
5 Minute Input Rate(packets/sec)	Input rate in 5 minute on this interface(packets/sec)				
5 Minute Input Rate(bits/sec)	Input rate in 5 minute on this interface(bits/sec)				
Unicast Packets	Total unicast packets received on this interface				
Broadcast Packets	Total broadcast packets received on this interface				
Multicast Packets	Total multicast packets received on this interface				
Runts	Total runts error packets received on this interface				
Giants	Total giants packets received on this interface				
Input Errors	Total input error packets received on this interface				
CRC	Total CRC error packets received on this interface				
Frame	Total frame packets received on this interface				
Overrun	Total overrun packets received on this interface				
Pause	Total pause packets received on this interface				
5 Minute Output Rate(packets/sec)	Output rate in 5 minute on this interface(packets/sec)				
5 Minute Output Rate(bits/sec)	Output rate in 5 minute on this interface(bits/sec)				
Unicast Packet	Total unicast packets transmitted on this interface				
Broadcast Packet	Total broadcast packets transmitted on this interface				
Multicast Packet	Total multicast packets transmitted on this interface				
Under runs	Total under runs packets transmitted on this interface				
Output Errors	Total output error packets transmitted on this interface				
Pause	Total pause packets transmitted on this interface				

3. Link Aggregation Configuration

3.1 Basic Information

If you click "Configuration -> Llink aggregation" in the top control bar, the link aggregation configuration list page appears, as shown in figure 1.

FS 55850-48T4Q		Monitor	Configuration	X Maintenance	Network	Save	admin	Logou
🐨 Ethernet Status	Global Link Ag	gregation	1					
Inik Aggregation 2 Storm Control 2	Global * Load Balance Mode	Destination MAC Address						
Flow Control Port Isolate		Source MAC Address Control of the second se						
 Port Detect VLAN 		Source IP Address IP Protocol Type Oestination Port						
Standard Classifier		Source Port						
열 Spanning Tree 성 ERPS		Inner Source MAC Address Inner Destination IP Address Inner Source IP Address						
田 Mirror 系 Multicast		Inner IP Protocol Type Inner Destination Port						
		Inner Source Port NVGRE VSID VXLAN VNI						
			Coj	oyright © Fiberstore . All F	lights Reserved.			

Figure 1 Link aggregation

This chapter describes the link aggregation configuration function and view the link aggregation information of the switch.

3.1.1 Basic Information(S5800-8TF12S)

The link aggregation function of device S5800-8TF12S is different from that of other devices. If you click "Configuration -> Llink aggregation" in the top control bar, the link aggregation configuration list page appears, as shown in figure 2.

FS [55800-81F125]	Monitor	Configuration	* Maintenance	Network			
Ithermet Status Clobal Lisk Aggregation It Storm Control Clobal Clobal It Storm Control Clobal -: Load Balance Mode It Not Control Clobal -: Load Balance Mode It NAN Clobal -: Load Balance Mode It VLAN Clobal -: Load Balance Mode It NAN Clobal -: Load Balance Mode It NANC Clobal <td< th=""><th>gregation Destination (IF Address Destination MIC Address Destination MIC Address Destination For Destination For Source and Destination (For Address Source Address Source FIX Address Source FIX Address Source FIX Address</th><th>1</th><th></th><th></th><th></th><th></th><th></th></td<>	gregation Destination (IF Address Destination MIC Address Destination MIC Address Destination For Destination For Source and Destination (For Address Source Address Source FIX Address Source FIX Address Source FIX Address	1					

Figure 2 Link aggregation

3.2 Link Aggregation Global Configuration

If you click "Llink aggregation -> Global" in the title bar, the link aggregation global configuration page appears, as shown in figure 3.

Ethernet Status 2 Global	Link Appreciation
United Status	enn riggragmen.
Storm Control	
* Load Bala	nce Mode Destination MAC Address
Port Isolate	Destination IP Address
Port Detect	Source IP Address
VLAN	Protocol type Destination Port
VLAN Classifier	Source Port
MAC	Inner Destination MAC Address
Spanning Tree	Inner Destination IP Address
C ERPS	Inner Source IP Address
Mirror	Inner IP Protocol Type Inner Destination Port
😤 Multicast	Inner Source Port
	NvGRE VSID
	VXLAN VNI

Figure 3 Link Aggregation global configuration information

Parameter usage

ltem	Description
Destination MAC address	Load balancing according to destination MAC
Source MAC address	Load balancing according to source MAC
Destination IP address	Load balancing according to destination IP
Source IP address	Load balancing according to source IP
IP Protocol Type	Load balancing according to IP protocol
Destination Port	Load balancing according to destination port
Source Port	Load balancing according to source port
Inner Destination MAC address	Load balancing according to destination MAC of inner layer message
Inner Source MAC address	Load balancing according to source MAC of inner layer message
Inner Destination IP address	Load balancing according to destination IP of inner layer message
Inner Source IP address	Load balancing according to source IP of inner layer message
Inner IP Protocol Type	Load balancing according to IP protocol of inner layer message
Inner Destination Port	Load balancing according to the destination port of inner layer message
Inner Source Port	Load balancing according to the source port of inner layer message
NvGRE VSID	Load balancing according to Negre's VSID
VxLAN VN	Load balancing according to VSID of Vxlan

If you want to configure the link aggregation global configuration, you can perform the following steps:(1) You can select the check box in the left column of the load balancing mode you want to configure.

(2) Then click the "Apply" button to configure the load balancing mode. The operation is shown in figure 4.

FS 55850-24T165		Monitor	Configuration	Maintenance	Network	
	Global Link A	ggregation				
🕑 Ethernet Status						
👾 Link Aggregation	Global					
X Storm Control	* Load Balance Mode	Destination MAC Address	1			
II Flow Control		Source MAC Address Destination IP Address				
Port Isolate		Source IP Address				
Port Detect		IP Protocol Type				
LL VLAN		Destination Port Secures Part				
88 VLAN Classifier		Inner Destination MAC Add	ress			
MAC		Inner Source MAC Address				
Spanning Tree		Inner Destination IP Address	5			
✓ ERPS		Inner Source IP Address Inner ID Protocol Turne				
I Mirror		Inner Destination Port				
& Multicact		Inner Source Port				
55 multicast		NVGRE VSID				
		VxLAN VNI				
		Apply 2				
			Соругі	ght © 2009-2020 FS.COM In	: . All Rights Reserved.	

Figure 4 Link Aggregation global configuration

3.2.1 Global Configuration(S5800-8TF12S)

If you click "Llink aggregation -> Global" in the title bar, the link aggregation global configuration page appears, as shown in figure 5.

Cobus Link Aggregation	
M Lok Ageregation 2 M Storm Control	

Figure 5 Load balance mode configuration

• Parameter usage

Item	Description
Destination IP address	Load balancing according to destination IP
Destination MAC address	Load balancing according to destination MAC
Destination Port	Load balancing according to destination port

FS



ltem	Description
Source and Destination IP address	Load balancing according to source IP address and destination IP address
Source and Destination MAC address	Load balancing according to source MAC address and destination MAC address
Source and Destination Port	Load balancing according to source port and destination port
Source IP address	Load balancing according to source IP
Source MAC address	Load balancing according to source MAC
Source Port	Load balancing according to source port

If you want to configure the link aggregation global configuration, you can perform the following steps:

You can select the radio box in the left column of the load balancing mode you want to configure.
 Then click the "Apply" button to configure the load balancing mode.
 The operation is shown in figure 6.



Figure 6 Link Aggregation global configuration

3.3 Link Aggregation Configuration

If you click "Llink aggregation -> Link aggregation" in the title bar, the link aggregation configuration page appears, as shown in figure 7.

🖲 Ethernet Status	Global Link Aggregation	2				
Image: Storm Control Image: Storm Control	Link Aggregation Add Delete Refr	esh				
Port Isolate	Link Aggregation Name	Protocol	Group State	Ports In Bundle	Ports	Operation
Port Detect	agg10	Static	12	0	2	Edit
La VLAN						
B8 VLAN Classifier						
MAC						
🛱 Spanning Tree						
4¢ ERPS						
I Mirror						
🖧 Multicast						

Figure 7 Link aggregation configuration information

Parameter usage

ltem	Description
Link Aggregation Name	Display the name of link aggregation interface
Protocol	Display link aggregation protocol mode
Group State	Display the group state of link aggregation interface
Ports in Bundle	Display the current ports number in bundle
Ports	Display the link aggregation member ports
Operation	Modify the configuration of this link aggregation group

3.3.1 User Configuration Add Link Aggregation

If you click "Add", you can add link aggregation, as shown in figure 8, and then the link aggregation configuration page appears, as shown in figure 9.

Global	Link Aggregation					
Link Aggrega	Delete Refresh					
Link A	ggregation Name	Protocol	Group State	Ports In Bundle	Ports	Operation
agg10		Static	L2	0	2	Edit

Figure 8 Add link aggregation operation

D concerner of a constant						
🙀 Link Aggregation	LAG Name	AGG Please	enter the age	regation group	o number	
34 Storm Control	LAG Member Port	🗌 eth-0-1	🗌 eth-0-2	🗌 eth-0-3	🗌 eth-0-4	🗌 eth-0-5
Flow Control		🗍 eth-0-6	eth-0-7	🗌 eth-0-8	🗌 eth-0-9	🗌 eth-0-10
Port Isolate		🗌 eth-0-11	🗌 eth-0-12	🗌 eth-0-13	🗌 eth-0-14	🗌 eth-0-15
Port Detect		🗌 eth-0-16	🗌 eth-0-17	🗌 eth-0-18	🗌 eth-0-19	🗌 eth-0-20
L VLAN		eth-0-21	i eth-0-22	(_) eth-0-23] eth-0-24	🗌 eth-0-25
VLAN Classifier		🗌 eth-0-26	🗌 eth-0-27	🗌 eth-0-28	🗌 eth-0-29	🗌 eth-0-30
MAC		eth-0-31	🗋 eth-0-32	🗌 eth-0-33	🗌 eth-0-34	🗋 eth-0-35
열 Spanning Tree		🗌 eth-0-36	🗌 eth-0-37	🗌 eth-0-38	🗌 eth-0-39	🗌 eth-0-40
4 ERPS		Apply	Back			
Mirror						
S Multicast						

Figure 9 Link aggregation configuration

Parameter usage

Item	Description
LAG Name	Display the name of link aggregation interface
LAG Member Port	Display the member port of link aggregation interface

If you want to add link aggregation, you can perform the following steps: (1) Fill LAG name.

Select LAG member port.
 Click "Apply" button to apply all the changes made.
 The operation is shown in figure 10, and the entry of the link aggregation configuration success table is shown in figure 11.

Static Link Aggregation							1
* LAG Name	1	AGG 1					(0-63)
* LAG Member Port	2	🔽 eth-0-1	🖌 eth-0-2	🗌 eth-0-3	🗌 eth-0-4	🗌 eth-0-5	
		eth-0-6	🗌 eth-0-7	eth-0-8	🗌 eth-0-9	🗌 eth-0-10	
		🗌 eth-0-11	🗌 eth-0-12	🗌 eth-0-13	🗌 eth-0-14	🗌 eth-0-15	
		eth-0-16	eth-0-17	🗌 eth-0-18	🗌 eth-0-19	🗌 eth-0-20	
		🗌 eth-0-21	🗌 eth-0-22	🗌 eth-0-23	🗌 eth-0-24	🗌 eth-0-25	
		🗌 eth-0-26	🗌 eth-0-27	🗌 eth-0-28	🗌 eth-0-29	🗌 eth-0-30	
		🗌 eth-0-31	eth-0-32	🗌 eth-0-33	🗌 eth-0-34	🗌 eth-0-35	
		🗌 eth-0-36	eth-0-37	🗌 eth-0-38	🗌 eth-0-39	🗌 eth-0-40	
	3	Apply	Back				

Figure 10 User configuration add link aggregation

Figure 11 New link aggregation information

3.3.2 User Configuration Edit Link Aggregation

If you click "Edit", you can edit link aggregation, as shown in figure 12, and then the link aggregation configuration page appears, as shown in figure 13.

Global	Link Aggregation					
Link Aggregati	On Delete Refresh					
🗋 Link Age	gregation Name	Protocol	Group State	Ports In Bundle	Ports	Operation
🗋 agg1		Static	L2	0	2	Edit



* LAG Name	AGG 1					(0-63)
* LAG Member Port	🗌 eth-0-1	deth-0-2	🗌 eth-0-3	🗌 eth-0-4	🗌 eth-0-5	
	eth-0-6	eth-0-7	eth-0-8	🗌 eth-0-9	🗌 eth-0-10	
	🗌 eth-0-11	eth-0-12	🗌 eth-0-13	🗌 eth-0-14	🗌 eth-0-15	
	🗌 eth-0-16	eth-0-17	eth-0-18	🗌 eth-0-19	🗌 eth-0-20	
	🗌 eth-0-21	🗌 eth-0-22	🗌 eth-0-23	🗌 eth-0-24	🗌 eth-0-25	
	eth-0-26	eth-0-27	eth-0-28	🗌 eth-0-29	🗌 eth-0-30	
	🗌 eth-0-31	🗌 eth-0-32	🗌 eth-0-33	🗌 eth-0-34	🗌 eth-0-35	
	🗌 eth-0-36	eth-0-37	🗌 eth-0-38	🗌 eth-0-39	🗌 eth-0-40	
	Apply	Back				

Figure 13 Link aggregation configuration edit

Parameter usage

ltem	Description
LAG Name	Display the name of link aggregation interface
LAG Member Port	Display the member port of link aggregation interface

If you want to edit link aggregation, you can perform the following steps:

Select LAG member port. (1)

(2) Click "Apply" button to apply all the changes made.
 The operation is shown in figure 14, and the entry of the link aggregation configuration success table is shown in figure 15.

Static Link Aggregation						
* LAG Name	AGG 1					(1-55)
* LAG Member Port	□ eth-0-1	✓ eth-0-2	✓ eth-0-3	🗌 eth-0-4	🗌 eth-0-5	
	🗌 eth-0-6	🗌 eth-0-7	🗌 eth-0-8	eth-0-9	🗌 eth-0-10	
	eth-0-11	eth-0-12	eth-0-13	eth-0-14	🗌 eth-0-15	
	eth-0-16	eth-0-17	🗌 eth-0-18	🗌 eth-0-19	🗌 eth-0-20	
	2 Apply	Back				

Figure 14 User edit a link aggregation configuration

Global	Link Aggregation					
Link Aggree	ation					
Add	Delete Refresh					
🗌 Link	Aggregation Name	Protocol	Group State	Ports In Bundle	Ports	Operation
🗆 aggʻ	ĺ.	Static	L2	0	2	Edit

Figure 15 New link aggregation information

3.3.3 Delete A Link Aggregation

If you want to delete the specified link aggregation, you can perform the following steps:

- You can select the check box in the left column of the link aggregation you want to delete. Then click the "Delete " button to delete the link aggregation. (1)
- (2)

Global Link Agg	regation				
Link Aggregation 2 Add Delete	Refresh				
Link Aggregation M	Name Protocol	Tine	P	orts	Operation
1 🗹 agg1	Static	TIPS	1		Edit
agg10	Static		2		Edit
		Are you sure to delete the selecte group data? Confirm Cancel	kd aggregate		

Figure 16 Delete a link aggregation

4. Storm Control

4.1 Storm Control

This section mainly describes how to configure and view interface storm control.

4.1.1 Basic Information

If you click "Configuration -> Storm Control" to check each interface storm control on switch, the configuration page is shown as the figure below.

FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network		Save admi	in Logout
Ethernet Status Link Aggregation	Storm Control		1					
Storm Control 2	Interface Name	Unicast Mode	Unicast Value	Broadcast Mode	Broadcast Value	Multicast Mode	Multicast Value	Operation
15 Flow Control	🗋 eth-0-1	disable		disable		disable		Edit
Dort Isolate	eth-0-2	disable		disable		disable		Edit
Port Detect	🔲 eth-0-3	disable		disable		disable		Edit
님 VLAN	🗌 eth-0-4	disable		disable		disable		Edit
B VLAN Classifier	🗋 eth-0-5	disable		disable		disable		Edit
MAC	🗌 eth-0-6	disable		disable		disable		Edit
🗄 Spanning Tree	eth-0-7	disable		disable		disable		Edit
48 ERPS	🗌 eth-0-8	disable		disable		disable		Edit
I Mirror	🗌 eth-0-9	disable		disable		disable		Edit
용 Multicast	eth-0-10	disable		disable		disable		Edit
🙊 QOS	eth-0-11	disable		disable		disable		Edit
🖄 ACL	eth-0-12	disable		disable		disable		Edit

Copyright © 2009-2020 FS.COM Inc . All Rights

Figure 1 Storm control basic information

Parameter usage

ltem	Description
Interface Name	Display the name of interface
Unicast Mode	Display the unicast storm control mode
Unicast Value	Display the unicast storm control value.Level: 0.00-100.00, PPS: 0-1000000000
Broadcast Mode	Display the broadcast storm control mode
Broadcast Value	Display the broadcast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Multicast Mode	Display the multicast storm control mode
Multicast Value	Display the multicast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Operation	Display that interface entries can be edited

4.1.2 Storm Control Attribute Configuration

In the Storm Control basic information page, If you choose one interface, and then click the "Edit" button, the operation is shown in figure 2. and then the interface storm control attribute configuration page appears, as shown in figure 3.

			Configuration	Maintenance	Network			
Ethernet Status Z Link Aggregation	n Control							
X Storm Control	Interface Name	Unicast Mode	Unicast Value	Broadcast Mode	Broadcast Value	Multicast Mode	Multicast Value	Operation
Flow Control	2 eth-0-1	disable		disable		disable		Edit
🕀 Port Isolate	2 eth-0-2	disable		disable		disable		Edit
D Port Detect] eth-0-3	disable		disable		disable		Edit
님 VLAN] eth-0-4	disable		disable		disable		Edit
88 VLAN Classifier] eth-0-5	disable		disable		disable		Edit
MAC] eth-0-6	disable		disable		disable		Edit
留 Spanning Tree] eth-0-7	disable		disable		disable		Edit
4¢ ERPS	eth-0-8	disable		disable		disable		Edit
@ Mirror	eth-0-9	disable		disable		disable		Edit
🖧 Multicast	eth-0-10	disable		disable		disable		Edit
A QOS	eth-0-11	disable		disable		disable		Edit
C ACL	eth-0-12	disable		disable		disable		Edit

Figure 2 Select the interface

FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network	Save admin Logout
😇 Ethernet Status	Storm Control					
帥 Link Aggregation	Interface Name	eth-0-1,eth-0-2				
X Storm Control	Unicast Mode	Disable O PPS	() Level			
Flow Control	Unicast Value	Please enter unicast val	lue		PPS: 0-1000000000 multiples of 10000, Level: 0.00-100.0	
Port Detect	Broadcast Mode	Disable O PPS	⊖ Level			
Li VLAN	Broadcast Value	Please enter broadcast	value		PPS: 0-1000000000 multiples of 10000, Level: 0.00-100.0	
BO VLAN Classifier	Multicast Mode	Disable O PPS	O Level			
☐ MAC	Multicast Value	Please enter multicast v	value		PPS: 0-1000000000 multiples of 10000, Level: 0.00-100.0	
Spanning Tree		Apply Back				
Mirror						
and Multicast						
🙉 qos						
🖾 ACL						
			Copyright	t © 2009-2020 FS.COM	Inc . All Rights Reserved.	

Figure 3 Interface storm control attribute configuration

• Parameter usage

ltem	Description
Interface Name	Display the name of interface
Unicast Mode	Enter the unicast storm control mode
Unicast Value	Enter the unicast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Broadcast Mode	Enter the broadcast storm control mode
Broadcast Value	Enter the broadcast storm control value. Level: 0.00-100.00, PPS: 0-1000000000
Multicast Mode	Enter the multicast storm control mode
Multicast Value	Enter the multicast storm control value. Level: 0.00-100.00, PPS: 0-1000000000

FS

4.1.3 Unknown Unicast Storm Control

FS 55800-8TF125		Monitor Configura	tion Maintenance	Network	Save admin Lo
Ethernet Status	Storm Control				
🕸 Link Aggregation	Interface Name	eth-0-1,eth-0-2			
X Storm Control					
Flow Control	 Unicast Mode 	Disable O PPS O Level			
🕒 Port Isolate	Unicast Value	Please enter unicast value		PPS: 0-1000000000 multiples of 10000, Level: 0.00-100.00)	
Port Detect	* Broadcast Mode	Disable O PPS O Level			
U VLAN	Broadcast Value	Please enter broadcast value			
8 VLAN Classifier	 Multicast Mode 	● Disable ○ PPS ○ Level			
MAC	Multicast Value	Please enter multicast value		PS: 0-100000000 multiples of 10000, Level: 0.00-100.00)	
🛱 Spanning Tree		Apply Back			
ko ERPS		(1997) Louis			
Hirror					
Pa Multicast					
a qos					
ACL					
			Copyright D 2009-2020 FS.COM (nc . All Rights Reserved.	

Figure 4 Setting the unknown unicast storm control

Through the radio buttons in the "Unicast Mode" bar, you can choose Disable/PPS/level. When you choose the PPS or level, in the "Unicast Value" bar, you can enter the value of the unicast packets. The legal threshold range for each port is given behind the threshold. Then click apply to apply all the changes made.

4.1.4 Broadcast Storm Control

FS 55800-8TF125		Monitor (Configuration	X Maintenance	A Network			
	Storm Control							
Ethernet Status M Link Aggregation	Interface Name	eth-0-1,eth-0-2						
X Storm Control	• Unicast Mode	Disable OPPS OLe	evel					
Flow Control	Unicast Value	Please enter unicast value						
Port Isolate	* Broadcast Mode	Disable OPPS OLe	evel					
LI VLAN	Broadcast Value	Please enter broadcast value			(PPS: 0-1000000000 multiples of 10000, Level: 0.00-10	0.00)		
B8 VLAN Classifier	+ Multicast Mode	Disable OPPS OLe	evel					
MAC	Multicast Value	Please enter multicast value						
Spanning Tree		Apply Back						
Mirror								
$d_{ab}^{\mathbb{Q}}$ Multicast								
A QOS								
2 ACL								
			Copyright 🕲 2	009-2020 FS.CO	vl Inc . All Rights Reserved.			

Figure 5 Setting the broadcast storm control

Through the radio buttons in the "Broadcast Mode" bar, you can choose Disable/PPS/level. When you choose the PPS or level, in the "Broadcast Value" bar, you can enter the value of the Broadcast packets. The legal threshold range for each port is given behind the threshold. Then click apply to apply all the changes made.

4.1.5 Multicast Storm Control

FS 55800-8TF125		Monitor	Configuration	X Maintenance	A Network	Save admin Logout
Ethernet Status	Storm Control					
帅 Link Aggregation	Interface Name	eth-0-1,eth-0-2				
X Storm Control	Unicast Mode	Disable O PPS	⊖ Level			
How Control	Unicast Value	Please enter unicast value				
Port Isolate Port Detect	Broadcast Mode	Disable OPPS	O Level			
님 VLAN	Broadcast Value	Please enter broadcast va	alue		(PPS: 0-1000000000 multiples of 10000, Level: 0.00-100.00)	
B8 VLAN Classifier	* Multicast Mode	Disable OPPS	O Level			
MAC	Multicast Value	Please enter multicast val	lue		(PPS: 0-1000000000 multiples of 10000, Level: 0.00-100.00)	
留 Spanning Tree		Apply Back)			
🦧 ERPS						
I Mirror						
Sh Multicast						
🕼 QOS						
🖄 ACL						
			Copyright	© 2009-2020 FS.COM	Inc . All Rights Reserved.	

Figure 6 Setting the multicast storm control

Through the radio buttons in the "Multicast Mode" bar, you can choose Disable/PPS/level. When you choose the PPS or level, in the "Multicast Value" bar, you can enter the value of the Multicast packets. The legal threshold range for each port is given behind the threshold. Then click apply to apply all the changes made.

5. Flow Control

FS S5800-8TF12S		Monitor	Configuration	Maintenance	Network		Save	admin Log
Ethernet Status Link Aggregation	Flow Control Display							
Storm Control	Interface Name	Receive Admin	Receive Operation	Send Admin	Send Operation	RxPause	TxPause	Operatio
Flow Control 2	🗋 eth-0-1	off	off	off	off	0	0	Edit
Port Isolate	eth-0-2	off	off	off	off	0	0	Edit
Port Detect	🗌 eth-0-3	off	off	off	off	0	0	Edit
L VLAN	🗌 eth-0-4	off	off	off	off	0	0	Edit
VLAN Classifier	eth-0-5	off	off	off	off	0	0	Edit
MAC	eth-0-6	off	off	off	off	0	0	Edit
Spanning Tree	eth-0-7	off	off	off	off	0	0	Edit
© ERPS	eth-0-8	off	off	off	off	0	0	Edit
1 Mirror	eth-0-9	off	off	off	off	0	0	Edit
& Multicast	🗌 eth-0-10	off	off	off	off	0	0	Edit
QOS	eth-0-11	off	off	off	off	0	0	Edit
] ACL	eth-0-12	off	off	off	off	0	0	Edit
					r. All Rights Reserved			

If you click "Configuration -> Flow Control" in the top control bar, the flow control page appears, as shown in figure 1.

Figure 1 Flow control page

This section mainly describes how to configure and view flow control.

5.1 Flow Control Display

If you click "Configuration -> Flow Control", the flow control display page appears, as shown in figure 2.

Edit Refresh							
Interface Name	Receive Admin	Receive Operation	Send Admin	Send Operation	RxPause	TxPause	Operation
🗌 eth-0-1	off	off	off	off	0	0	Edit
🗌 eth-0-2	off	off	off	off	0	0	Edit
🗌 eth-0-3	off	off	off	off	0	0	Edit
🗌 eth-0-4	off	off	off	off	0	0	Edit
eth-0-5	off	off	off	off	0	0	Edit
🗌 eth-0-6	off	off	off	off	0	0	Edit
🗌 eth-0-7	off	off	off	off	0	0	Edit
eth-0-8	off	off	off	off	0	0	Edit
🗌 eth-0-9	off	off	off	off	0	0	Edit
🗌 eth-0-10	off	off	off	off	0	0	Edit
🗌 eth-0-11	off	off	off	off	0	0	Edit
🗌 eth-0-12	off	off	off	off	0	0	Edit

Figure 2 Flow control display

This figure displays all interface name and their receiving and sending status.

Parameter usage

ltem	Description
Interface Name	Display the name of Interface
Receive admin	Display Receive configuration

Receive oper	Display Receiving status
Send admin	Display Send configuration
Send oper	Display Send status
RxPause	Display receive statistics
TxPause	Display Send statistics
Operation	Display that flow control table entries can be edited

5.2 Edit Flow Control

You can choose the check box in the left-hand column of flow control display page, then click "Edit" button, or directly click the "Edit" button in the right-most "Operation" bar, the operation is shown in figure 3, then port configuration page appears, as shown in figure 4.

Flo	·low Control Display							
2	Edit Refresh							
	Interface Name	Receive Admin	Receive Operation	Send Admin	Send Operation	RxPause	TxPause	Operation
	eth-0-1	off	off	off	off	0	0	Edit
1	eth-0-2	off	off	off	off	0	0 1	Edit
	🗋 eth-0-3	off	off	off	off	0	0	Edit
	🗌 eth-0-4	off	off	off	off	0	0	Edit
	🗌 eth-0-5	off	off	off	off	0	0	Edit
	🗌 eth-0-6	off	off	off	off	0	0	Edit
	🗌 eth-0-7	off	off	off	off	0	0	Edit
	🗌 eth-0-8	off	off	off	off	0	0	Edit

Figure 3 Edit flow control operation

Flow Control Configurat	ion
Interface Name	eth-0-2
Receive	⊖ On
Send	◯ On
	Apply Back

Figure 4 Port configuration list


Parameter usage

ltem	Description	
Receive	Receive status of current port flow control	
Send	Send status of current port flow control	

If you want to modify the sending and receiving status of flow control on the current port, such as enable flow control receive function and disable flow control send function, you can follow the following steps:

Click the "On" button in the line of "Receive" function. Click the "Down" button in the line of "Send" function. (1)

(2)

(3) Click the "Apply" button to modify the sending and receiving status of the current port.

The operation is shown in figure 5, modify the sending and receiving status of flow control on the current port configuration success table entry is shown in figure 6.

Flow Control Configurat	ion
Interface Name	eth-0-2
Receive	1 On Off
Send	On Off 2
	3 Apply Back

Figure 5 Edit flow control operation

Flow Control Display							
Interface Name	Receive Admin	Receive Operation	Send Admin	Send Operation	RxPause	TxPause	Operation
🗋 eth-0-1	off	off	off	off	0	0	Edit
🗋 eth-0-2	on	off	off	off	0	0	Edit
🗌 eth-0-3	off	off	off	off	0	0	Edit

Figure 6 New flow control information



6. Port Isolate

If you click "Configuration->Port Isolate" in the top control bar, the port isolate configuration list page appears, as shown in figure 1.

FS 55800-8TF125	Monitor Maintenance Network Save admin Lo	ogout
Ethernet Status Eink Aggregation Storm Control Flow Control Port isolate 2	Global Port Isolate Global * Port Isolate Mode @ 12AllApply	
	Figure 1 Port isolate configuration list	

This chapter describes how to configure port isolation and view port isolation group information.

6.1 Global Configuration

Port isolation provides two modes of operation, layer 2 isolation mode and layer 2 & 3 full isolation mode.

6.1.1 Current Port Isolation Mode

If you click "Port Isolate -> Global" in the title bar, the port isolation mode information page appears, as shown in figure 2.

Ethernet Status	2 Global Port Isolate
🚧 Link Aggregation	
🕱 Storm Control	Global
1 Flow Control	
Port Isolate 1	Арріу



Parameter usage

ltem	Description	
Port Isolate Mode	Display the mode of port isolation	

If you want to modify the mode of port isolation, please select layer 2 isolation mode or layer 2 & 3 full isolation mode, and then click the "Apply" button, the operation shown in figure 3.

Global Port Is	olate				
Global					
Port Isolate Mode	€L2 ○AII	1			
	Apply	2			

Figure 3 Select the isolation mode

6.2 Port Isolate Configuration

Through the port isolate configuration function, you can add ports to the isolation group, or remove ports from the isolation group, or modify the isolation group that ports join.

6.2.1 Port Isolate Group Information

If you click "Port Isolate -> Port Isolate" in the title bar, the port isolate group information page appears, as shown in figure 4.

Ethernet Status	Global Port Isolate 2	
Link Aggregation		
Storm Control	Port Isolate	
Flow Control	Edit	
Port Isolate	Interface Name Port Isolate Group	Operation
Port Detect	□ eth-0-1	Edit
VLAN	□ eth-0-2	Edit
3 VLAN Classifier	c eth-0-3	Edit
MAC	c eth-0-4	Edit
Spanning Tree	eth-0-5	Edit
ERPS	□ eth-0-6	Edit
Mirror	eth-0-7	Edit
a Multicast	eth-0-8	Edit
QOS	eth-0-9	Edit
ACL	C eth-0-10	Edit

Figure 4 Port isolate group information

Parameter usage

É

ltem	Description	
Interface Name	Display the name of interface	
Port Isolate Group	Display Specify the port isolate group	

6.2.2 Join the Port Isolation Group

If you first select the port to join the port isolation group, and then click "Edit" button, you can add ports to a port isolation group, the operation is shown in figure 5. And then configure the port to join the isolation group page to appear, as shown in figure 6.

Global Port Isolate		
ort Isolate		
Edit Refresh		
Interface Name Port Isolate Gr	oup	Operation
🗌 eth-0-1		Edit
eth-0-2		Edit
🗌 eth-0-3		Edit
v eth-0-4		Edit
✓ eth-0-5		Edit
v eth-0-6		Edit
	Figure 5 Add port to join the isolation group operation	
ort Isolate Management		
Interface Name	eth-0-4,eth-0-5,eth-0-6	
Port Isolate Enable	O Enable O Disable	

Figure 6 Add port to join the isolation group

• Parameter usage



ltem	Description
Interface Name	Display the ports to be added to the port isolation group
Port Isolate Enable	Set whether port isolation is enabled
Port Isolate Group	Set the number to join the port isolation group

If you want to add ports to the port isolation group, you can follow the following steps: (1) Enable port isolate in the "Port Isolate Enable" radio box.

- (2) Enter the port isolation group ID in the "Port Isolate Group" textbox.

Click the "Apply" button. (3)

The operation is shown in figure 7, the port successfully joined the isolation group's table entry information is shown in figure 8.

Interface Name	eth-0-4,eth-0-5,eth-0-6	
Port Isolate Enable	1 <u>Enable</u> O Disable	
Port Isolate Group	2 11	(1-31)
	3 Apply Back	

Figure 7 Port join the isolation group operation

Global	Port Isolate		
Port Isolate	Refresh		
Interface	Name	Port Isolate Group	Operation
🗌 eth-0-1			Edit
🗌 eth-0-2			Edit
🗌 eth-0-3			Edit
🗌 eth-0-4		11	Edit
🗌 eth-0-5		11	Edit
🗌 eth-0-6		11	Edit

Figure 8 New port isolation group information

6.2.3 Remove the Port Isolation Group

If you select the port of the isolation group first, and then click "Edit" button, you can remove ports from the isolation group, the operation is shown in figure 9. And then the page that configured the port to be removed from the isolation group appears, as shown in figure 10.

Global Port Isolate		
Port Isolate		
Interface Name	Port Isolate Group	Operation
🗋 eth-0-1		Edit
🗌 eth-0-2		Edit
🗌 eth-0-3		Edit
□ eth-0-4	11	Edit

Figure 9 Configure the port to remove the isolation group operation

Interface Name	ath 0.4	
interface Nume.	etti-0-4	
Port Isolate Enable	● Enable ○ Disable	
Port Isolate Group	11	(1-31)

Figure 10 Remove port isolation group information

Parameter usage

ltem	Description	
Interface Name	Display the ports on which the isolation group will be removed	
Port Isolate Enable	Set whether port isolation is enabled	
Port Isolate Group	Set the number to join the port isolation group	

If you want to remove ports from the isolation group, you can disable port isolate in the "Port Isolate Enable" radio box, and then click the "Apply" button, the operation is shown in figure 11, the port was successfully removed from the isolation group is shown in figure 12.

Port Isolate Management		
Interface Name	eth-0-4	
Port Isolate Enable	⊖ Enable	
Port Isolate Group	Please enter the port isolation group	(1-31)
2	Apply Back	
	Figure 11 Port removal isolation group operation	
Global Port Isolate		
Port Isolate		
Edit Refresh		
Interface Name Port Isolate Group		Operation
🗌 eth-0-1		Edit
C eth-0-2		Edit
🗌 eth-0-3		Edit
eth-0-4		Edit



6.2.4 Modify the Port Isolation Group

If you select the port of the isolation group first, and then click "Edit" button, you can modify the ports to join the port isolation group, the

operation is shown in figure 13. And then the modify port isolation group configuration page appears, as shown in figure 14.

Global	Port Isolate	
Port Isolate	Refresh	
Interface	Name Port Isolate Group	Operation
eth-0-1		Edit
eth-0-3		Edit
eth-0-5	11	Edit



Port Isolate Management

Interface Name	eth-0-5	
Port Isolate Enable	● Enable ◯ Disable	
Port Isolate Group	11	(1-31)
	Apply Back	

Figure 14 Modify port isolation group information

Parameter usage

ltem	Description	
Interface Name	Displays the port to modify the isolation group	
Port Isolate Enable	Set whether port isolation is enabled	
Port Isolate Group	Set the number to join the port isolation group	

If you want to modify the port isolation group id, you can modify the port isolation group id in the "Port Isolate Group" textbox, and then click the "Apply" button to modify port isolation group, the operation is shown in figure 15, the isolation group id of the port was modify successfully is shown in figure 16.

Port Isolate Managemer	t		
Interface Name	eth-(0-5	
Port Isolate Enable	1 O Ena	ble 🔿 Disable	
Port Isolate Group	2 12		(1-31)
	3 🗛	ply Back	

Figure 15 Modify the port isolation group operation

Global Port Isolate		
Port Isolate		
Interface Name	Port Isolate Group	Operation
🗋 eth-0-1		Edit
🗌 eth-0-2		Edit
🗌 eth-0-3		Edit
🗌 eth-0-4		Edit
🗍 eth-0-5	12	Edit

Figure 16 Port isolation group information

6.2.5 Refresh the Port Isolation Group

If you want to refresh the port isolation group configuration information, you can click "Refresh" button. The operation is shown in figure 17.

Global Port I	solate	
Port Isolate	esh	
🗌 Interface Name	Port Isolate Group	Operate
🔲 eth-0-1		Edit

Figure 17 Refresh the port isolation group configuration information

7. Port Detect

If you click "Configuration -> Port Detect" in the top control bar, the port detect page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	Maintenance Retwork	Save admin Logout
Ethernet Status Link Aggregation Storm Control Control	Params Configuration Link-flap * Counts 100	(1-100, Default 10)	+ Seconds 120	(1-120, Default 10)
Port Isolate Port Detect 2 VLAN	Fbd-loop * Count 50 Recovery time	(3-50, Default 10)	Exclude-vlan	(1-4094,eg-2-5,7,9-11 Default N/A)
VLAN Classifier MAC Conserving Tags	* Seconds 86400	(30-86400, Default 300)		
Spanning ree ERPS Mirror	Detect Configuration Reason	Detect	Recovery	
A Multicast	Bpduguard Fdb-loop	Enabled	Disabled Disabled Disabled	
Z ACL	Link-flap	Enabled T	Disabled *	

Figure 1 Port detect page

Port detect can detect the link error status of the port.

7.1 Parameter Configuration

7.1.1 Basic Information

If you click "Configuration -> Port Detect", the parameter configuration list appears, as shown in figure 2.

ink-flap			
Counts	10	* Seconds	10
	(1~100, Defa	ult 10)	(1~120, Default 10
bd-loop			
Count	10	Exclude-vlan	
	(3~50, Defa	ult 10)	(1~4094,eg:2-5,7,9-11 Default N/A
ecovery time			
Seconds	300		
	(30~86400, Defaul	t 300)	

Figure 2 Parameter configuration list

• Parameter usage

Item	Description
Link-flap	Display Link flapping detection
Counts	Display the number of link flapping detection
Seconds	Display the link flapping detection period in seconds

ltem	Description
Fdp-loop	Display FDB for check function
Count	The number of FDB drifts detected during the period
Exclude-vlan	Set the list of VLAN that FDB does not detect
Recovery time	Interval to recover from error state
Seconds	Display the number of intervals to recover from an error state

7.1.2 Modify Parameter Configuration

If you want to modify parameter configuration, you can follow the following steps:

- Enter the number of times to modify link flapping detection in the "counts" text box. (1)
- (2)
- Enter the link flapping detection period in the "Seconds" text box. Enter the number of FDB drifts to be detected during the period in the "Count" text box. (3)
- (4) Set the list of VLAN not detected by FDB in the "Exclude-vlan" text box.
- Set the number of time intervals to recover from the error state in the "Seconds" text box. (5)
- (6) Click the "Apply" button to modify parameter configuration.

NOTE: The items with the asterisk symbol "*" are ones where you must enter values.

The operation is shown in figure 3, modify parameter configuration success table entry is shown in figure 4.

Params Configura	tion							
Link-flap								
* Counts	50	(1~100, Default 10)	* Seconds 2	60		(1~120, Del	fault 10)	
Fbd-loop								
* Count	20	3	Exclude-vlan 4	2				
Recovery time								
* Seconds	500	5						
		(30~86400, Default 300)						
Detect Configurat	ion							
Reason		Detect		Recovery				
Bpduguard		Enabled		Disabled	•			
Fdb-loop		Disabled 🔻		Disabled	•			
Bpduloop		Enabled		Disabled	•			
Link-flap		Enabled 🔻		Disabled	•			
Link-monitor-	failure	Enabled		Disabled	•			
Udld		Disabled 🔻		Disabled	•			
Loopback-det	ection	Enabled		Disabled	*			
Monitor-link		Enabled		N/A				
Oam-remote-	failure	Enabled		Disabled	•			
Reload-delay		Enabled		N/A				
Port-security		Enabled		Disabled	•			
Apply	5							

Figure 3 Parameter configuration operation

Params Configura	ition		
Link-flap			
* Counts	50	* Seconds	60
	(1~100, Default 10)		(1~120, Default 10)
Fbd-loop			
* Count	20	Exclude-vlan	2
	(3~50, Default 10)		(1~4094,eg:2-5,7,9-11 Default N/A)
Recovery time			
* Seconds	500		
	(30~86400, Default 300)		

Figure 4 New parameter configuration

7.2 Detect Configuration

If you click "Configuration -> Port Detect", the detect configuration list appears, as shown in figure 5.

FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network	Save admin Logout
	Detect Configuration					
😳 Ethernet Status	Reason	Detect		Recovery		
00 Link Aggregation	Bpduguard	Enabled		Disabled	•	
🕱 Storm Control	Fdb-loop	Disabled	•	Disabled	•	
Flow Control	Bpduloop	Enabled		Disabled	•	
Port Isolate	Link-flap	Enabled	•	Disabled	•	
Port Detect	Link-monitor-failure	Enabled		Disabled	*	
L VLAN	Udld	Disabled	•	Disabled	•	
BB VLAN Classifier	Loopback-detection	Enabled		Disabled	•	
MAC	Monitor-link	Enabled		N/A		
🖺 Spanning Tree	Oam-remote-failure	Enabled		Disabled	•	

Figure 5 Detect configuration list

You can enable or disable error recovery for specific reasons in this list.

|--|

ltem	Description
Bpduguard	Display Enable recovery from BPDU guard error state
Fdb-loop	Display Enable FDB loop recovery function
bpduloop	Display enable BPDU loopback error status recovery function
link-flap	Display the function of link flapping error recovery
link-monitor-failure	Display enable link monitoring error recovery
udid	Display enable UDLD error recovery function
loopback-detection	Display enable loopback detection error status recovery function
monitor-link	Display enable link monitoring recovery function
oam-remote-failure	Display enable recovery from OAM error
Reload-delay	Display enable reload delay function
Port-security	Display enable port binding error recovery

7.2.1 Modify Error Recovery Function

If you want to modify enable or disable error recovery function, such as enable fdb-loop and link-flap error recovery function, you can follow the following steps:

- Select the enable of the drop-down box of the recovery bar corresponding to fdb-loop. (1)
- Select the enable of the drop-down box of the recovery bar corresponding to link-flap. Click the "Apply" button to modify error recovery function. (2)

(3)

The operation is shown in figure 6, modify error recovery function success table entry is shown in figure 7.

Detect Configuration			
Reason	Detect	Recovery	
Bpduguard	Enabled	Disabled *	
Fdb-loop	Disabled •	Enabled T	
Bpduloop	Enabled	Disabled 🔻	
Link-flap	Enabled	Enabled T	
Link-monitor-failure	Enabled	Disabled	
Udld	Disabled 🔻	Disabled 💌	
Loopback-detection	Enabled	Disabled T	
Monitor-link	Enabled	N/A	
Oam-remote-failure	Enabled	Disabled 🔻	
Reload-delay	Enabled	N/A	
Port-security	Enabled	Disabled 🔹	



Figure 6 Modify error recovery function operation

Det	tect Configuration		
	Reason	Detect	Recovery
	Bpduguard	Enabled	Disabled 💌
	Fdb-loop	Disabled 🔻	Enabled 💌
	Bpduloop	Enabled	Disabled 💌
	Link-flap	Enabled 🔻	Enabled 💌
	Link-monitor-failure	Enabled	Disabled •
	Udld	Disabled 🔻	Disabled 🔻
	Loopback-detection	Enabled	Disabled *
	Monitor-link	Enabled	N/A
	Oam-remote-failure	Enabled	Disabled 💌
	Reload-delay	Enabled	N/A
	Port-security	Enabled	Disabled 💌

Figure 7 New detect configuration list

8. VLAN

8.1 VLAN

VLAN (Virtual Local Area Network) means logically dividing a LAN (Local Area Network) into many different subsets, and each subset will form its own broadcast domain. In short, VLAN is a telecommunication technology dividing a physical LAN into many broadcast domains. The hosts in VLAN can directly communicate with each other, while VLANs can not directly intercommunicate. Therefore, the broadcast message is limited in a VLAN. The network security is improved.

If you click "Configuration ->VLAN" in the top control bar, the VLAN configuration list page appears, as shown in figure 1.

FS 55800-8TF125		Mon	2 iitor	Configuration	X Maintenance	A Network	Save ad	lmin Logou
				1				
🖱 Ethernet Status	VLAN Summary	VLAN Interface	Access/Trunk	Port				
00 Link Aggregation	~							
🕱 Storm Control	VLAN Summary							
1 Flow Control	VLAN Add/Delete	Refresh						
🖶 Port Isolate	VLAN ID Status	MAC Learning	Action	Limit	Member Port		Description	Operation
Port Detect					eth-0-1(t) eth-0-2(u) eth-0-8(u) eth	eth-0-3(u) eth-0-4(u) eth-0-5(u) eth-0-6(u) eth- n-0-9(u) eth-0-10(u) eth-0-11(u) eth-0-12(u) eth-		
WLAN 2	1 Active Enable	Forward N/A	N/A	0-13(u) eth-0-14(u) agg2(u) agg3(u)	0-13(u) eth-0-14(u) eth-0-15(u) eth-0-16(u) eth-0-20(u) agg1(u) agg2(u) agg3(u)	default	Edit	
BB VLAN Classifier								
MAC	Total 1 records.						10 🔻	*
딸 Spanning Tree								
d₀ ERPS								
I Mirror								
😤 Multicast								
🚇 QOS								
ACL								
				Copyrigh	nt @ 2009-2020 FS.COM Inc.	All Rights Reserved.		

Figure 1 VLAN configuration list

This section describes VLAN configuration function and viewing VLAN information of the switch.

8.1.1 Basic Information

If you click "VLAN > VLAN Summary" in the title bar, the VLAN summary page appears, as shown in figure 2.

LAN Summar	у						
VLAN Add	d/Delete	Refresh					
VLAN ID	Status	MAC Learning	Action	Limit	Member Port	Description	Operation
1	Active	Enable	Forward	N/A	eth-0-1(u) eth-0-2(u) eth-0-3(u) eth-0-4(u) eth-0-5(u) eth-0-6(u) eth-0-7(u) eth-0-8(u) eth-0-9(u) eth-0-10(u) eth-0-11(u) eth-0-12(u) eth-0-13(u) eth-0-14(u) eth-0-15(u) eth-0-16(u) eth-0-17(u) eth-0- 18(u) eth-0-19(u) eth-0-15(u) eth-0-16(u) eth-0-17(u) eth-0-	default	Edit

Figure 2 VLAN summary information

Parameter usage

ltem	Description
VLAN ID	Display the number of interface
Status	Display the status of VLAN

Replace DSCP	Display the replace DSCP of VLAN						
MAC Learning	Display the MAC learning status of VLAN						
Action	Display the action mode of VLAN						
Limit	Display the mac-limit maximum of VLAN						
Member Port	Display the member port of VLAN						
Description	Description about the VLAN						
Operate	Display that interface entries can be edited						

8.1.2 Add or Delete VLAN

If you click "VLAN add/delete" button, you can add add/delete VLAN, the operation is shown in figure 3. And then the add VLAN & VLAN range settings page appears, as shown in figure 4.

VLAN Summar	y VLA	N Interface	Access/Trunk	Port			
/LAN Summa	ry d/Delete	Refresh					
VLAN ID	Status	MAC Learning	Action	Limit	Member Port	Description	Operation
1	Active	Enable	Forward	N/A	eth-0-1(u) eth-0-4(u) eth-0-5(u) eth-0-6(u) eth-0-7(u) eth-0-8(u) eth-0-9(u) eth-0-10(u) eth-0-11(u) eth-0-12(u) eth-0-13(u) eth-0- 14(u) eth-0-15(u) eth-0-16(u) eth-0-17(u) eth-0-18(u) eth-0-19(u) eth-0-20(u) agg1(u)	default	Edit
Total 1 recor	ds.					10 💌	→

Figure 3 Add or delete VLAN operation

igure Mode	Single	
LAN ID	Please enter VLAN ID	(2-4094)
escription	Please enter description	

Figure 4 Add/Delete VLAN & VLAN range settings

Parameter usage

ltem	Description				
Configure Mode	Display specify VLAN add mode				
VLAN ID	Display the number of interface (rang 2-4994)				
Description	Description about the VLAN				



Operate

Display that interface entries can be edited

If you want to add/delete VLAN, you can follow the following steps:

- Select the configure mode. Enter VLAN ID. (1)
- (2)
- (3) Enter Description.
- Click the "Add"/"Delete" button to apply all the changes made. (4)

The operation is shown in figure 5, VLAN configuration success table entry is shown in figure 6.

Add/Delete VLAN & VLAN Range Settings

Configure Mode	Single	•	1
VLAN ID	10		(2-4094)
Description	vlan10		
4	Add Delete Back		



VLAN Summar	N VLA	N Interface	Access/Trunk I	Port			
VLAN Summa	ify id/Delete	Refresh					
VLAN ID	Status	MAC Learning	Action	Limit	Member Port	Description	Operation
1	Active	Enable	Forward	N/A	eth-0-1(u) eth-0-2(u) eth-0-3(u) eth-0-4(u) eth-0-5(u) eth-0-6(u) eth-0-7(u) eth-0-8(u) eth-0-10(u) eth-0-11(u) eth-0-12(u) eth-0-13(u) eth-0-14(u) eth-0-15(u) eth-0-16(u) eth-0-17(u) eth-0- 18(u) eth-0-19(u) eth-0-20(u)	default	Edit
10	Active	Enable	Forward	N/A	N/A	vlan10	Edit

Figure 6 New VLAN information

8.1.3 Modify VLAN

If you want to modify a VLAN, please click "Edit" button, the operation shown in figure 7, VLAN detailed configuration page appears, as shown in figure 8.

VLAN Summ	nary VL	AN Interface	Access/Trunk	Port			
VLAN Summ	nary Add/Delete	Refresh					
VLAN ID	Status	MAC Learning	Action	Limit	Member Port	Description	Operation
t	Active	Enable	Forward	N/A	eth-0-1(u) eth-0-2(u) eth-0-3(u) eth-0-4(u) eth-0-5(u) eth-0-6(u) eth-0-7(u) eth-0-8(u) eth-0-9(u) eth-0-10(u) eth-0-17(u) eth-0-12(u) eth-0-13(u) eth-0-14(u) eth-0-15(u) eth-0-16(u) eth-0-17(u) eth-0-18(u) eth-0-19(u) eth-0-20(u) eth-0-18(u) eth-0-17(u) eth-0-18(u) eth-0-19(u) eth-0-19(u) eth-0-18(u) eth-0-17(u) eth-0-18(u) et	default	Edit
10	Active	Enable	Forward	N/A	N/A	vlan10	Edit
Total 2 record	ls.					10 💌	+

Figure 7 Modify VLAN operation

VLAN Detailed Configuration

VLAN ID	10				
Member Port					
VLAN State	Enable	⊖ Disable			
Replace DSCP	Disable				
Mac Learning	O Enable	⊖ Disable			
Mac Limit Action	⊖ Discard	Forward	⊖ Warn		
Mac Limit Max Number	0				(0~65535. default 0,0 means no limit)
Description	vlan10				
	Apply	Back			

Figure 8 VLAN detailed configuration

• Parameter usage

ltem	Description					
VLAN ID	Display the number of interface					
Member Port	Display the member port of VLAN					
VLAN Status	Display the status of VLAN					
Replace DSCP	Display the replace DSCP of VLAN					
MAC Learning	Display the MAC learning status of VLAN					
Mac Limit Action	Display the action mode of VLAN					
Mac Limit Max Number	Display the mac-limit maximum of VLAN					
Description	Description about the VLAN					

If you want to modify a VLAN detail, you can follow the following steps:
(1) Choose VLAN state.
(2) Choose MAC Learning.

- (3)
- Choose Mac Limit Action. Modify the mac-limit maximum of VLAN. (4)
- (5) Modify the description about the VLAN.
 (6) Click the "Apply" button to apply all the changes made. The operation is shown in figure 9.

AN Detailed Configura	tion	
VLAN ID	10	
Member Port		
VLAN State	◯ Enable	
Replace DSCP	Disable	
Mac Learning	◯ Enable	
Mac Limit Action	● Discard ○ Forward ○ Warn 3	
Mac Limit Max Number	6000	(0~65535. default 0,0 means no limit)
Description	vlanfs	5
6	Apply Back	

Figure 9 Modify VLAN detailed configuration

8.2 VLAN Interface

VLAN interface: a logical interface with three layers of characteristics, through the configuration of VLANIF interface IP address, VLAN visits.VLAN interfaces can be created and deleted.

Through the VLAN interface configuration function, you can add/modified/delete the VLAN interface on switch.

8.2.1 VLAN Interface Information

If you click "VLAN -> VLAN Interface" in the title bar, the VLAN Interface page appears, as shown in figure 10.

FS SS800-8TF12S		Monitor	Configuration	Maintenance	Network	Save admin Log	gout
			1				
Ethernet Status	VLAN Summary 3 VLAN In	terface Access/	Trunk Port				
🕸 Link Aggregation							
3 Storm Control	VLAN IF Interface						
1 Flow Control	Add Delete Re	efresh					
Port Isolate	ULAN Interface Name	IPv4 Address				Operatio	ion
Port Detect	Ulanif1	192.168.1.119/24				Edit	
H VLAN 2							
B8 VLAN Classifier							
MAC							
😫 Spanning Tree							
48 ERPS							
Mirror							
🖧 Multicast							
A QOS							

Figure 10 VLAN interface

Parameter usage

ltem	Description
VLAN interface Name	Display Layer 3 VLAN interface name
IPv4 Address	Set the IP address of an interface
Operate	Display that interface entries can be edited

8.2.2 Add VLAN IF

If you click "New" button, you can add a VLAN IF, the operation is shown in figure 11. and then the VLAN Interface Management page appears, as shown in figure 12.

FS 55800-8TF125		Monitor	Configuration	Maintenance	network	Save admin Logout
Fill Ethernat Status	VI AN Summary	fare Arress/	in mk Port			
Einer Status Einer Aggregation	(Citrodinity)	nice in the state of the state				
3 Storm Control	VLAN IF Interface					
E Flow Control	Add Delete Kette	sn				
Port Isolate	VLAN Interface Name	IPv4 Address				Operation
Port Detect	C	100.00011103/27				Eun

Figure 11 Add VLAN IF operation

VLAN Interface Manag	gement	
VLAN Interface ID	Please enter ID	(1-4094)
IPv4 Address	a a a	
MASK	0.0.0(0)]
	Apply Back	

Figure 12 VLAN interface management

Parameter usage

ltem	Description
VLAN interface ID	Display Layer 3 VLAN interface name
IPv4 Address	Set the IP address of an interface
Mask	IP subnet mask

If you want to add the VLAN IF, you can follow the following steps:

- Enter a VLAN id in the "VLAN interface ID" textbox, but you should first create a VLAN which you want to use. Enter IP address in the "IPv4 Address" textbox. (1)
- (2)
- (3) Select the destination address mask in the "mask " dropdown box.
- Click the "Apply" button to apply all the changes made. (4)

The operation is shown in figure 13, route configuration success table entry is shown in figure 14.

VLAN Interface ID	10	(1-4094)
IPv4 Address	192 . 168 . 1 . 110	
MASK	255.255.255.0(24)	*

Figure 13 Add VLAN IF configuration



💬 Ethernet Status	VLAN Summary VLAN Interface Access/Trunk Port	
🔶 Link Aggregation		
I Storm Control	VLAN IF interface	
Flow Control	Add Dedete Refresh	
🕀 Port Isolate	VLAN interface Name IPv4 Address	Operation
Port Detect	Viaift	Edit
H VLAN	Uanif100 192.168.1.110/24	Edit
88 VLAN Classifier		
MAC MAC		

Figure 14 New VLAN IF information

8.2.3 Delete VLAN IF

If you want to delete the specified VLAN IF, you can follow the following steps:

(1) select this specified VLAN IF which you want to delete.

(2) click "Delete" button.

(3) confirm the selected delete VLAN IF and page appears as shown in figure 15, if you click "Confirm" button, you can delete this VLAN IF.

VLAN Summary	VLAN Interface Access/True	nk Port		
VLAN IF Interface	elete			
VLAN interface	ce Name IPv4 Address	tips	×	Operation
Vlanif1		693		Edit
1 Vlanif100	192.168.1.110/24			Edit
		Are you sure to delete selected Vlan	n Interface?	
		3 Confirm Cancel		

Figure 15 Delete VLAN IF

8.3 Acess/Trunk Port

8.3.1 Acess /Trunk Port Basic Information

If you click "VLAN > Access/Trunk Port" in the title bar, the access/trunk port page appears, as shown in figure 16.

			_			
Ethernet Status	VLAN Summary VLAN Inter	face 2 Access/Trunk Port]			
🚸 Link Aggregation			-			
3 Storm Control	Access/Trunk Port					
Flow Control	Edit					
Port Isolate	Interface Name	Mode	Ingress Filtering	PVID	Add VLAN	Operation
🗁 Port Detect	🗌 eth-0-1	access	enable	1	1	Edit
H VLAN 1	□ eth-0-2	access	enable	1	1	Edit

Figure 16 Access/Trunk port information

Parameter usage

Item	Description
Interface Name	Display the name of interface
Mode	Indicate VLAN membership mode for an interface Access: set the port as an Access VLAN interface. The port transmits tagged or untagged frames on a single VLAN only Trunk: specify an interface as VLAN Trunk interface. A trunk is a direct link between two switches, so the interface transmits tagged frames marked the source VLAN. Note that frames belonging to the interface's default VLAN are also transmitted as untagged frames

Ingress Filtering	Determine how to process the tagged frame, which is not included in this VLAN. (Default: Enable) Ingress filtering only affects tagged frames. If ingress filtering is disabled and the interface receives a tagged frame which is not included in this VLAN, these frames will be flooded to all other ports within this VLAN If ingress filtering is enabled and the interface receives a tagged frame, which is not included in this VLAN, then the frame will be dropped
PVID	Display the native VLAN ID of interface
AddVLAN	If the displayed link type is Trunk, VLAN ID or list is allowed to pass through the interface If the displayed link type is Access, the VLAN ID that the interface belongs to, and the tagged or untagged frames received on the interface will be tagged with the VLAN ID (default: 1)
Operate	Display that interface entries can be edited

8.3.2 Access/Trunk Port Modification

If you want to modify the configuration to specify access/trunk port, please click "Edit" button in the operation bar, or you can follow the following steps:

(1) Select this interface which you want to edit.

(2) Click "Edit" button. the operation is shown in figure 17. and then the access/trunk port modification page appears, as shown in figure 18.

Operation
Edit

Figure 17 Access/Trunk port edit operation

Access/Trunk Port Modification				
* Interface Name	eth-0-1			
* Interface Mode	access			
* PVID	1	(1-4094)		
* Permit VLAN	1	(1~4094), example: 2-5,7		
	Apply Back			

Figure 18 Access/Trunk port modification

Parameter usage



ltem	Description
Interface Name	Display the name of interface
Interface Mode	Indicate VLAN membership mode for an interface Access: set the port as an Access VLAN interface. The port transmits tagged or untagged frames on a single VLAN only Trunk: specify an interface as VLAN Trunk interface. A trunk is a direct link between two switches, so the interface transmits tagged frames marked the source VLAN. Note that frames belonging to the interface's default VLAN are also transmitted as untagged frames
Ingress Filtering	Determine how to process the tagged frame, which is not included in this VLAN. (Default: Enable) Ingress filtering only affects tagged frames. If ingress filtering is disabled and the interface receives a tagged frame which is not included in this VLAN, these frames will be flooded to all other ports within this VLAN If ingress filtering is enabled and the interface receives a tagged frame, which is not included in this VLAN, then the frame will be dropped
PVID	Display the native VLAN ID of interface



ltem	Description
Permit VLAN	If the displayed link type is Trunk, VLAN ID or list is allowed to pass through the interface If the displayed link type is Access, the VLAN ID that the interface belongs to, and the tagged or untagged frames received on the interface will be tagged with the VLAN ID (default: 1)
Operate	Display that interface entries can be edited

If you want to modify an access/trunk port, you can follow the following steps:
(1) Modify PVID in the "PVID" textbox.
(2) Modify Permit VLAN in the "Permit VLAN" textbox.
(3) Click the "Apply" button to modify the specify static route.
The operation is shown in figure 19.

Note: When the port mode is trunk, you can select the progress filtering able or disable.

Ethernet Status	Access/Trunk Port M	odification	
00 Link Aggregation	Interface Name	eth-0-1	
IX Storm Control			
E Flow Control	Interface Mode	access	
Port Isolate	1 • PVID	1	(1-4094)
Port Detect			 1
H VLAN	2 * Permit VLAN	1	(1-4094), example: 2-5,7
BB VLAN Classifier	3	Apply Back	
MAC MAC			
留 Spanning Tree			
dan ERPS			
Mirror			
and Multicast			
A QOS			
🖄 ACL			

Figure 19 Modify an access/trunk port configuration

9. VLAN Classifier

If you click "Configuration -> VLAN Classifier" in the top control bar, the VLAN classifier configuration page appears, as shown in figure 1.

FS 55800-8TF12S		Monitor	Configuration	X Maintenance	Retwork		
Ethernet Status Hink Aggregation Storm Control	VLAN Classifier Rules Add Delete Refresh Refresh	Ru	1 le Type	F	tule Content	VID	
 Flow Control Port Isolate Port Detect VLAN VLAN Classifier 2 VLAN Spanning Tree ERPS Mirror 	VI AN Classifier Grouns			No Data-			
A Multicast	Add Delete Refresh		Rule ID				
			Copyright	© 2009-2020 FS.COM Inc	. All Rights Reserved.		

Figure 1 VLAN classifier list

This section mainly describes how to configure and view VLAN classifier.

9.1 VLAN Classifier Rules

If you click "Configuration -> VLAN Classifier", the VLAN classifier rules list appears, as shown in figure 2.

AN Classifier Rules	sh			
Rule ID	Rule Type	Rule Content	VID	
		No Data~		

Figure 2 VLAN classifier rules List

• Parameter usage

ltem	Description			
Rule ID	Display the ID of Rule			
Rule Type	Display the Type of Rule, including IP, MAC and protocol			
Rule Content	Display the IP address of the current rule			
VID	Display the VLAN ID of interface.			

9.1.1 Add VLAN Classifier Rules

If you click "Add" in the VLAN classifier rules list, you can add a VLAN classifier rule, the operation is shown in figure 3, then VLAN classifier rule settings page appears, as shown in figure 4.

VLAN Cla 1 Ad	Delete Refresh			
R	ule ID	Rule Type	Rule Content	VID



Figure 3 Add VLAN classifier rules operation

/lan Classifier R	ule Settings	
Rule ID		(0-4095)
Rule Type	IP	~
IP Address		(0.0.0)
Vlan ID		(1-4094)
	Apply Back	

Figure 4 VLAN classifier rule settings list

• Parameter usage

ltem	Description		
Rule ID	Display the ID of Rule		
Rule Type	Display the Type of Rule, including IP, MAC and protocol		
IP Address	IP address for which classification rules need to be set		
VLAN ID	Display the VLAN ID of interface		
IP	IP-based VLAN are classified based on the source IP address of incoming packets		
МАС	MAC-based VLAN are classified based on the source MAC address of incoming packets		
protocol	Protocol-based VLAN are classified based on Layer 3 protocol type incoming packets		

If you want to add a VLAN classifier rule, you can follow the following steps:

- (1) Enter a rule ID in the range of 0-4095.
- (2) Select IP/ MAC/ protocol from the "Rule Type" drop-down box.
- (3) Enter a valid IP address in the "IP Address" text box.
- (4) Enter the VLAN ID in the range of 1- 4094.
- (5) Click the "Apply" button to add a VLAN classifier rule.

The operation is shown in figure 5, add a VLAN classifier rule configuration success table entry is shown in figure 6.

Vlan Classifier Rule Settings





VLAN Classifier Rules				
Add Delete Refresh				
Rule ID	Rule Type	Rule Content	VID	
3	ip	192.168.1.3	3	

Figure 6 New VLAN classifier rule information

9.1.2 Delete VLAN Classifier Rules

If you want to delete the specified VLAN classifier rule, you can follow the following steps: (1) Choose the check box in the left-hand column of the specified VLAN classifier rule.

- (2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button, it will delete this VLAN classifier rule;
 If you click "cancel" button, you will cancel delete this VLAN classifier rule operation, as shown in figure 7.

ou chek	currect	button, you will cance	at classifier i	raie operation, a	sinominingare	<i>'</i> .

FS 55800-8TF125		Monitor Configuration	K II Maintenance Network	Save admin
🗇 Ethernet Status	VLAN Classifier Rules			
00 Link Aggregation	Add Delete Refresh			
💢 Storm Control	Rule ID	Rule Type	Rule Content	VID
Elow Control	1 🛃 3	ip	192.168.1.3	3
Port Isolate		tips	×	
Port Detect	VLAN Classifier Groups			
∐ VLAN	Add Delete Refresh)		
B8 VLAN Classifier	Group ID		e you sure to delete selected classifier rule?	
MAC				
留 Spanning Tree		3	Confirm	
do ERPS				
I Mirror				
$\mathbb{P}_{d \in \mathbb{N}}$ Multicast				
a qos			No Data~	
Z ACL				
		Copyright	© 2009-2020 F5.COM Inc . All Rights Reserved.	

Figure 7 Delete VLAN classifier rule operation

Delete a VLAN classifier rule configuration success table entry is shown in figure 8.

AN Classifier Rules				
Add Delete Refresh				
Rule ID	Rule Type	Rule Content	VID	
		No Data -		

Figure 8 Delete VLAN classifier rule information

9.2 VLAN Classifier Groups

If you click "Configuration -> VLAN Classifier", the VLAN classifier groups list appears, as shown in figure 9.



Figure 9 VLAN classifier groups list

9.2.1 Add VLAN Classifier Groups

If you click "Add" in the VLAN classifier groups list, you can add a VLAN classifier group, the operation is shown in figure 10, then the VLAN classifier groups settings page appears, as shown in figure 11.



Figure 10 Add VLAN classifier group operation

Apply

Vlan Classifier	Group Settings —		
Group ID			
Rule ID			

Back

Figure 11 VLAN classifier group settings list

Parameter usage

Item	Description
Group ID	Set the ID of Group
Rule ID	Set the ID of Group

If you want to add a VLAN classifier group, you can follow the following steps:

- (1) Enter a group ID in the range of 0-31.
- (2) Enter a rule ID in the range of 0- 4095, the rule ID must exist in the VLAN classifier rules list.
- (3) Click the "Apply" button to add a VLAN classifier group.

NOTE: Different types of VLAN classifier rules can be added to the same VLAN classification group.

The operation is shown in figure 12, add a VLAN classifier group configuration success table entry is shown in figure 13.

lan Classifier (Group Settings		
Group ID	1	(0-31)	1
Rule ID	3	(0-4095)	2
3	Apply Back		

Figure 12 Add VLAN classifier group operation

/LAN Classifier Groups	
Add Delete Refresh	
Group ID	Rule ID
0 1	1
8 1	2
1	3

Figure 13 New VLAN classifier group information

9.2.2 Delete VLAN Classifier Groups

If you want to delete a specified VLAN classifier group, you can follow the following steps:

(1) Choose the check box in the left-hand column of the specified VLAN classifier group.

(2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button, it will delete this VLAN classifier group; If you click "cancel" button, you will cancel delete this VLAN classifier group operation, as shown in figure 14.

3	ip	tips	3
VLAN Classifier Groups		Are you sure to delete selected Classifier Gro	pup?
Group ID 2		RL 3 Confirm Cancel	
		2	
		3	

Figure 14 Delete VLAN classifier group operation

Delete a VLAN classifier group configuration success table entry is shown in figure 15.

Add Delete Refresh		
Group ID	Rule ID	
1	1	
1	2	

Figure 15 Delete VLAN classifier group

9.3 VLAN Classifier Usage

If you click "Configuration -> VLAN Classifier", the VLAN classifier usage list appears, as shown in figure below.

Add Delete Refresh		
Interface	Group ID	Based Type
1	1	2
⊒ 1	1	2

Figure 16 VLAN classifier usage list

9.3.1 Add VLAN Classifier Usage

If you click "Add" in the VLAN classifier usage list, you can add a VLAN classifier usage, the operation is shown in figure 17, then VLAN classifier usage settings page appears, as shown in figure 18.

VLAN Classifier Usage Add Delete Refresh		
Interface	Group ID	Based Type
1	1	2
D 1	1	2

Figure 17 Add VLAN classifier usage operation

Vlan Classifier U	lsage Settings		
Interface	eth-0-1	•	
Group ID	1	•	
Based Type	ip	•	
	Apply Back		

Figure 18 VLAN classifier usage settings list

Parameter usage

ltem	Description
Interface	Select an interface to apply VLAN classification
Group ID	Select a Group ID exist in the VLAN Classifier Groups list
Base Type	Choose what type of interface to base on, including IP mac and protocols

If you want to add a VLAN classifier usage, you can follow the following steps:

- (1) Select port from the "Interface" drop-down box.
- (2) Select a group ID from the drop-down box, the group ID has been created in the VLAN classifier groups list.
- (3) Select IP /MAC/protocol from the "Based Type" drop-down box.
- (4) Click the "Apply" button to add a VLAN classifier usage.

The operation is shown in figure 19, add a VLAN classifier usage configuration success table entry is shown in figure 20.

Interface	eth-0-5	-
Group ID	1	•
Based Type	ip	~

Figure 19 Add VLAN classifier usage operation

VLAN Classifier Usage Add Delete Refresh		
Interface	Group ID	Based Type
1	1	2
□ 1	1	2
□ eth-0-5	1	ip

Figure 20 New VLAN classifier usage information

9.3.2 Delete VLAN Classifier Usage

If you want to delete a specified VLAN classifier usage, you can follow the following steps:

- (1) Choose the check box in the left-hand column of the specified VLAN classifier usage.
- (2) Click "Delete" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button, it will delete this VLAN classifier usage; If you click "cancel" button, you will cancel delete this VLAN classifier usage operation, as shown in figure 21.

· · · · · · · · · · · · · · · · · · ·		
Add Delete Refresh	tips ×	
Group ID	RL	
□ 1	1 Are you sure to delete selected Classifier Interface?	
B 1	2	
	3 Confirm cancel	
VLAN Classifier Usage		
Add Delete Refresh		
Interface 2	Group ID	Based Type
1	1	2
0 1	1	2
eth-0-5 1	1	ip

Figure 21 Delete VLAN classifier usage operation

Delete a VLAN classifier usage configuration success table entry is shown in figure 22.



VLA	N Classifier Groups	
	Add Delete Refresh	
	Group ID	Rule ID
	1	1
	■ 1	2

Figure 22 Delete VLAN classifier group

10. MAC

If you click "Configuration->MAC" in the top control bar, the MAC configuration list page appears, as shown in figure 1.

FS 55800-8TF125		Monitor I	Configuration	Maintenance	Network	Save admin Logout
Ethernet Status	MAC Address Table MAC	ilobal Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security Static Security MAC
00 Link Aggregation						
X Storm Control	Mac Address Table Information					
Flow Control	MAC Type All			▼ MAC Address		
Port Isolate	VLAN Please Enter VLAN			Interface Type All		*
Port Detect			(1-4094)			
L VLAN	Interface Name All			Query		
B VLAN Classifier	MAC Address	VLAN		Interfa	ce	Entry Type
MAC 2	6499.9910.3365	1		eth-0-5	5	dynamic
留 Spanning Tree	649d.9910.0ad2	1		eth-0-5	5	dynamic
48 ERPS	3c2c.30f2.9df0	1		eth-0-5	5	dynamic
Mirror	3c2c.30e1.b244	1		eth-0-5	5	dynamic
$\partial_{\delta}^{\mathcal{Q}}$ Multicast	b05c.da37.e702	1		eth-0-5	5	dynamic
A QOS	8cec.4bc5.e472	1		eth-0-5	5	dynamic
🖄 ACL	3c2c.30f2.9584	1		eth-0-5	S	dynamic
					All Rights Reconvert	

Figure 1 MAC configuration list

Ethernet switch uses information of MAC address list to address and forward the message quickly in link data layer, this article describes the configuring methods of MAC address.

10.1 MAC Address Table

MAC address table allows checking MAC address forwarding table of switch, if switch learns a MAC address and its relevant interface number, it will create an entry in forwarding table, these entries are used in forwarding packets. if the destination address of inbound traffic is in the database, the packets will be directly forwarded to related interface, or they will be forwarded to all interfaces. If you click "Configuration > MAC > MAC Address Table" page to open the page as shown in following figure 2, which displays the address list information of switch.

FS 55800-81F125		Monitor 1	Configuration	% Maintenance	network			
😨 Ethernet Status	MAC Address Table 3 MAC	Slobal Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security S	itatic Security MAC	
(i) Link Aggregation	Mac Address Table Information							
Flow Control	MAC Type All			MAC Address				
Port Isolate	VLAN Please Enter VLAN		(1-4094)	Interface Type All		-		
U VLAN	Interface Name All			• Query				
BB VLAN Classifier	MAC Address	VLAN		Interfa	(e	Entry Type		
🖵 мас 2	6499.9910,3365	1		eth-0-5	i	dynamic		
🗒 Spanning Tree	649d.9910.0ad2	1		eth-0-5	i	dynamic		
48 ERPS	3c2c.30f2.9df0	1		eth-0-5	5	dynamic		
/ Mirror	3c2c.30e1.b244	1		eth-0-5	i	dynamic		
An Multicast	b05c.da37.e702	1		eth-0-5	6	dynamic		
@ QOS	8cec.4bc5.e472	1		eth-0-5	6	dynamic		
🖾 ACL	3c2c.30f2.9584	1		eth-0-5	ł.	dynamic		

Figure 2 MAC address table page

Parameter usage

ltem	Description
MAC Address	The MAC addresses in the address table
VLAN	VLAN ID that corresponds to the above MAC address

Interface	Interface that corresponds to the above MAC address
Entry Type	The methods that switch discovers MAC address, which includes Dynamic, Security or Station

If you want to view MAC address information for a MAC address table, you can follow the following steps:

(1) Select MAC address type in the "MAC type" drop-down box.

(2) Enter the MAC address to be queried in the "MAC address" text box.

- (3) Enter the VLAN number to be queried in the "VLAN" text box.
- (4) Select interface type in the "Interface type" drop-down box.
- (5) Select interface name in the "Interface name" drop-down box.
- (6) Click "Query" button, display the MAC address table information.

MAC Address Table MAC Global Configu	ration MAC Learning S	Static MAC Table Blackho	e MAC Table Port Security	Static Securi	by MAC	
Mac address table information 1		2			3	
MAC Type All	.*.	Mac address .	20		VLAN Please Enter VLAN	
Interface Type All	¥	Interface Name all		×	Query 6	
MAC address 4	VIAN	5	Interface		Entry Type	
0000.0000.0001	1		eth-0-1		static	
Total: 1 records.						10 💌 🔿

Figure 3 MAC address table information

10.2 MAC Aging Time

Use MAC aging time to set the remaining time of the learned MAC address in MAC address forwarding table, if exceeds this time, the switch will discard the MAC address forwarding records.

If you click "Configuration > MAC > MAC Global Configuration" page to view the configuration of MAC aging time, as shown in figure 4.

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network		Save admin Logout
🙂 Ethernet Status	MAC Address Table 3	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security	Static Security MAC
🕸 Link Aggregation	MAC Clabel Configuration						
30 Storm Control	IMAC Global Configuratio	m					
Flow Control	Aging Time	300					
Port Isolate		Apply					
Port Detect							
LE VLAN							
B8 VLAN Classifier							
₩AC 2							
B Spanning Tree							
< ERPS							
& Multicet							
20 ACI							
			Copyrig	ht © 2009-2020 FS.COM Inc	: All Rights Reserved.		
		Fig	ure 4 MAC a	aging time pa	age		

Parameter usage

Item	Description
Aging Time	Enter MAC address aging time(Range:0, 10~1000000 seconds; default: 300 seconds)

If you want to configure MAC aging time, please enter the aging time for mac address in the "Aging time" text box, then click" Apply" button, the operation is shown in figure 5.



Figure 5 MAC aging time configuration

10.3 MAC Learning

If you click "Configuration -> MAC -> MAC Learning" to check each interface MAC learning on switch, the configuration page is shown as the figure 6.

FS 55800-8TF12S		Monitor	Configuration	X Maintenance	Network		Save ad	
		_						
Ethernet Status	MAC Address Table MAC C	Global Configuration 3	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security	Static Security MAC	
00 Link Aggregation		L						
X Storm Control	MAC Learning							
E Flow Control	Edit Refresh							
Port Isolate	Interface Name	MAC Learning						Opreation
D Port Detect	🗌 eth-0-1	Enable						Edit
L VLAN	🗌 eth-0-2	Enable						Edit
88 VLAN Classifier	🗍 eth-0-3	Enable						Edit
⊊ MAC 2	🗌 eth-0-4	Enable						Edit
智 Spanning Tree	🗇 eth-0-5	Enable						Edit
48 ERPS	🗍 eth-0-6	Enable						Edit
I Mirror	eth-0-7	Enable						Edit
Pa Multicast	eth-0-8	Enable						Edit
🙉 QOS	c eth-0-9	Enable						Edit
ACL	- eth-0-10	Enable						Edit
								1101-01-01

Figure 6 MAC learning page

Parameter usage

ltem	Description
Interface Name	Display the name of interface
MAC Learning	Display the current MAC learning status on interface
Operation	Display that MAC learning status can be edited

If you want to modify the MAC learning, you can follow the following steps:

(1)

Click "Configuration -> MAC -> MAC Learning" to enter the basic information page. Choose one or more interface click "Edit" button to enter the interface attribute configuration page. (2)

- Select "Enable/Disable" in the "MAC learning" radio box. After that, click "Apply" to apply all the changes made.
- (3) (4)

FS [\$5800-8TF125]		Monitor	Configuration	X Maintenance	Network		Save as	lmin Logout
Thernet Status	MAC Address Table	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security	Static Security MAC	
🕸 Link Aggregation	MACLearning		1					
3% Storm Control	WAC Learning							
Flow Control	Edit							
Port Isolate	Interface Name	MAC Learning						Opreation
Port Detect	🗹 eth-0-1	Enable						2 Edit
H VLAN	🗋 eth-0-2	Enable						Edit
Bo VLAN Classifier	🗌 eth-0-3	Enable						Edit
MAC	🗌 eth-0-4	Enable						Edit
留 Spanning Tree	🔲 eth-0-5	Enable						Edit
🖑 ERPS	🗌 eth-0-6	Enable						Edit
Mirror	🗌 eth-0-7	Enable						Edit
$\delta^{\mathcal{P}_{h}}_{h}$ Multicast	🗌 eth-0-8	Enable						Edit
A QOS	🗌 eth-0-9	Enable						Edit
ACL	c eth-0-10	Enable						Edit

Figure 7 Interface MAC learning configuration



10.4 Static MAC Table

After the MAC address is bound to the assigned interface, the crated static MAC table entry will not be aging in the address table, if the address is discovered by another interface, it will be neglected and not be written into address table, the address will not be learned by other interfaces unless the static address is deleted manually from address table.

If you click "Configuration > MAC > Static MAC Table" page to open the page as shown in following figure 9, which displays the information of static address table of switch.

FS 55800-8TF12S		Monitor Configuration	Maintenance	Network		
III Etharnet Statur	MAC Address Table MAC Globa	Configuration MAC Learning	3	Blackhole MAC Table	Port Security Static Se	curity MAC
M Link Aggregation						
Storm Control	MAC Address		VLAN Please Ente	er VLAN		
Flow Control Port Isolate	Interface Type All		Interface Name All		(1-4094)	Query
Port Detect	New Delete					
≟≟ VLAN	MAC Address	VLAN	Interfa	ice	Entry Type	
88 VLAN Classifier	0100.5e7f.fffa	1	eth-0-	5	static	
Spanning Tree	Total: 1 records.					10 👻 👄
🐇 ERPS						

Figure 9 Static MAC table page

Parameter usage

ltem	Description
MAC Address	The MAC addresses in the address table
VLAN	VLAN ID that corresponds to the above MAC address
Interface	Interface that corresponds to the above MAC address
Entry Type	The methods that switch discovers MAC Static address

- If you want to add the static MAC address, you can follow the following steps:
 (1) Click "New" button to add a static MAC address, the configuration page is shown as the figure 10.
- (2) (3) Enter the MAC address to be added in the "MAC address" text box.
- Enter the VLAN number to be added in the "VLAN" text box.
- (4) Select interface type in the "Interface type" drop-down box.
- Select interface name in the "Interface name" drop-down box. After that, click "Apply" to apply all the changes made. (5)
- (6)

MAC Address Table	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security	Static Security MAC	
Static MAC Table							
Mac address			Vlan	ease Enter VLAN			
Interface Type All			Interface Nam	e All		(1-4094) Query	
New Delete							
1 MAC address		VIAN		Interface		Entry Type	

Figure 10 Add static MAC address

Static MAC Table

* Mac address	e e	2	
* VLAN	Please Enter VLAN	(1-40	194) 3
Interface Type	Ethernet	- 4	
Interface Name	eth-0-1	▼ 5	
	6 Apply Back		

Figure 11 Static MAC address configuration

If you want to delete the static MAC address, you can follow the following steps:

- (1) Click "Configuration -> MAC -> Static MAC Table" to enter the basic information page.
- (2) Choose the check box in the left-hand column of static MAC to be deleted, then click "Delete" button to delete static MAC entry.
- (3) It will appear tips page to note you to confirm the operation, if you click "Apply" button, it will delete the configuration for static MAC address table; if you click "cancel" button, you will cancel the delete configuration operation.

MAC Address Table MAC Global Configuration	MAC Learning	Static MAC Table Blackhole MAC Table	Port Security	Static Security MAC	
Static MAC Table		1			
Mac address		Vlan Please Enter VLAN			
				1094)	
Interface Type All		tips	×	Query	
New Delete 2					
MAC address	VIAN	Are you sure to delete selected MAC address	ss?	Entry Type	
፼ 0000.0000.0001	1	-		static	
Total: 3 records.		Apply Cancel			10 💌 🔿
		3			

Figure 12 Delete static MAC address

10.5 Blackhole MAC Table

If you click "Configuration > MAC > Blackhole MAC Table" page to open the page as shown in following figure 13, which displays the information of blackhole address table on switch.



Figure 13 Blackhole MAC table page

• Parameter usage

ltem	Description
MAC Address	The Blackhole MAC addresses in the address table
Entry Type	The methods that switch discovers MAC Static address

If you want to add a blackhole MAC adress, you can follow the following steps:

- (1) Click "New" button to add a blackhole MAC address, the configuration page is as shown in following figure 14.
- (2) Enter the blackhole MAC address information to be added in configuration page.
- (3) After that, click "Apply" to apply all the changes made.

MAC Address Table	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security	Static Security MAC
Riackhola MAC Table						
MAC Address			Query			
			query			
1 New Delete						
MAC Address		Entry Type				

Figure 14 Add blackhole MAC address

Blackhole MAC Table			
 Mac address 		2	
	Apply Back		
	3		


If you want to delete the blackhole MAC address, you can follow the following steps: (1) Click "Configuration -> MAC -> Blackhole MAC Table" to enter the basic information page.

- Choose the check box in the left-hand column of blackhole MAC to be deleted, then click "Delete" button to delete blackhole MAC (2) entry.
- (3) It will appear tips page to note you to confirm the operation, if you click "Apply" button, it will delete the configuration for blackhole MAC address table; if you click "cancel" button, you will cancel the delete configuration operation.



Figure 16 Delete blackhole MAC address

10.6 Port Security

If you click "Service Management -> MAC -> Port Security" to check each interface port security on switch, the configuration page is shown as the figure below 17.

FS 55800-87F125		Monitor	Configuration	X Maintenance	Network		we admin Logout
						3	
Ethernet Status	MAC Address Table	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security Static Securit	ty MAC
0 Link Aggregation							
11 Storm Control	Port Security						
Flow Control	Interface Name	Port Secu	rity	Interface P	rotect Mode	Maximum MAC addresses	Opreation
Port Isolate	eth-0-1	disable					Edit
Port Detect	eth-0-2	disable					Edit
H VLAN	eth-0-3	disable					Edit
88 VLAN Classifier	eth-0-4	disable					Edit
☐ MAC 2	eth-0-5	disable					Edit
留 Spanning Tree	eth-0-6	disable					Edit
4d ERPS	eth-0-7	disable					Edit
Mirror	eth-0-8	disable					Edit
and Multicast	eth-0-9	disable					Edit
🔱 QOS	eth-0-10	disable					Edit

Figure 17 Port security page

Parameter usage	
ltem	Description
Interface Name	Display the name of interface
Port Security	Display the current port security status on interface
Interface Protect Mode	Display the current protect mode on interface
Maximum MAC addresses	Display the maximum MAC addresses number on interface
Operation	Display that port security status can be edited

- If you want to modify the port security, you can follow the following steps:
 (1) Click "Configuration -> MAC -> Port Security" to enter the basic information page.
- (2) Choose one interface click "Edit" button to enter the interface attribute configuration page, shown as the figure 18.
- Select "Disable/Enable" in the "Port security" radio box. (3)
- (4) Select "Protect/Restrict/Shutdown" in the "Interface protect mode" radio box.
- Enter max MAC learn in the "Max MAC entries learned" text box. (5)
- (6) After that, click "Apply" to apply all the changes made.

MAC Address Table	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	1	Port Security	Static Security MAC	
Port Security								
Interface Name	P	Port Security		Interface Protect Mode			Maximum MAC addresses	Opreation
eth-0-1	d	lisable						2 Edit
eth-0-2	d	lisable						Edit
eth-0-3	d	lisable						Edit
eth-0-4	d	lisable						Edit
eth-0-5	d	lisable						Edit
eth-0-6	d	lisable						Edit
eth-0-7	d	lisable						Edit
eth-0-8	d	lisable						Edit
eth-0-9	d	lisable						Edit
eth-0-10	d	lisable						Edit

Figure 18 Port security information

Port Security			
Interface Name	eth-0-1		
Port Security	● Disable ○ Enable 1		
Interface Protect Mode	Protect Restrict Shutdown		
* Max MAC Entries Learned	1	(1~16384, Default 1) 3	
4	Apply Back		

Figure 19 Port security configuration

10.7 Static Security MAC

Static security MAC table lists the information of the static security MAC address among the switch interfaces.

If you click "Configuration > MAC > static security MAC" page to open the page as shown in following figure 20, which displays the information of static security address table of switch.

FS [55800-8TF125]		Monitor	X Maintenance		Save admin	Logout
Ethernet Status	MAC Address Table MAC Global C	Configuration MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security MAC 3	
辩 Link Aggregation	Shells County MAC Table					
🕅 Storm Control	Static Security MAC Table					
Flow Control	MAC Address .		VLAN Please Er	iter VLAN		
Port Isolate	Interface Type All		▼ Interface Name	All	Query	
D Port Detect	New					
님 VLAN						
BB VLAN Classifier	MAC Address	VLAN	In	iterface	Entry Type	
MAC 2						
Spanning Tree						
4 ERPS						
I Mirror						
\mathcal{L}^{Q}_{ab} Multicast			-			
🚇 QOS						
🖾 ACL			No Data~			
		Соруг	ight © 2009-2020 FS.COM Inc	. All Rights Reserved.		

Parameter usage

Item	Description
MAC Address	The MAC addresses in the address table
VLAN	VLAN ID that corresponds to the above MAC address
Interface	Interface that corresponds to the above MAC address
Entry Type	The methods that switch discovers MAC Static address

If you want to add the static security MAC address, you can follow the following steps:

- (1) Click "New" button to add a static MAC address, the configuration page is shown as the figure 21.
- (2) Enter the MAC address to be added in the "MAC address" text box.
- (3) Enter the VLAN number to be added in the "VLAN" text box.
- (4) Select interface type in the "Interface type" drop-down box.
- (5) Select interface name in the "Interface name" drop-down box.
- (6) After that, click "Apply" to apply all the changes made.

tic Security MAC Table Mac address , , Van Please Enter VLAN (1-009) Corry Detec MAC address VAN Interface Name Interface Entry Type	AC Address Table	MAC Global Configuration	MAC Learning	Static MAC Table	Blackhole MAC Table	Port Security	Static Security MAC	
Mac address Vian Prese Enter VIAN (1-030) Interface Type All Curry Ceter Mac address VIAN Interface Type Entry Type	ntic Security MAC Tab	le						
Interface Type All Interface Name All Carry MAC address VAN Interface Type	Mac address	e e		Vlan Plea:	e Enter VLAN			
New Delete MAC address VAN Interface Entry Type	nterface Type All			▼ Interface Name	All		Query	
MAC address VAN Interface Entry Type	New Delete							
	MAC address		VIAN		Interface		Entry Type	

Figure 21 Add static security MAC address

Mac address		2	
VLAN	Please Enter VLAN	(1-4094) 3	
nterface Type	Ethernet	- 4	
nterface Name	eth-0-1	. ₹	

Figure 22 Static security MAC address configuration

If you want to delete the static security MAC address, you can follow the following steps:

- (1) Click "Configuration -> MAC -> Static Security MAC Table" to enter the basic information page.
- (2) Choose the check box in the left-hand column of static MAC to be deleted, then click "Delete" button to delete static MAC entry.
- (3) It will appear tips page to note you to confirm the operation, if you click "Apply" button, it will delete the configuration for static security MAC address table; if you click "cancel" button, you will cancel the delete configuration operation.

MAC Address Table	MAC Global Configuration	MAC Learning	Static MAC Tab	le Blackhole MAC Table	Port Security	Static Security MAC	
Static Security MAC Tal	ble						
Mac address			Vlan	Please Enter VLAN		(1-4094)	
Interface Type All	2		tips		×	▼ Query	
MAC address		VIAN	🕕 Are y	ou sure to delete selected MAC address	?	Entry Type	
፼ 0000.0000.000	33	1				security	
Total: 1 records.				Apply Cancel			10 💌
				3			

Figure 23 Delete static security MAC address

11. Spanning Tree

Spanning Tree Protocol (STP) is used to decrease link failure in network and provides protection for network by preventing loop circuit. It is easy to generate unconscious loop broadcast storm in complex network construction. It is disabled by default. To enable this function, you must enable STP/RSTP/MSTP function on each switch connected to network. The switch supports three versions of Spanning Tree Protocol: STP, RSTP and MSTP.

If you click "Configuration -> Spanning Tree" the top control bar, the STP configuration page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network	Save admin	
Ethernet Status	STP Information GI	lobal Configuration	STP Ports MST Region				
🚸 Link Aggregation							
🕱 Storm Control	STP Information(RSTP MO	22768 (0+9000)					
Flow Control	Root ID Address	649d.9900.e4b1					
Port Isolate	Root ID Hello Time	2 sec					
D Port Detect	Root ID Max Age	20 sec					
⊥ VLAN	Root ID Forward Delay	15 sec					
00 VI AN Classifier	Root Path Cost	0					
aa VLAN Classiner	Bridge ID Priority	32768 (0x8000)					
MAC	Bridge ID Address	649d.9900.e4b1					
열 Spanning Tree 2	Bridge ID Helio Time	2 sec					
48 ERPS	Bridge ID Max Age	20 sec					
I Mirror	Bridge ID Aging Time	300 sec					
Sta Multicast	Edgeport bpdu-filter	Disabled					
🚇 QOS	Edgeport bpdu-guard	Enabled					
CT ACL	Priority Information						
			Copyright (2009-2020 FS.COM Inc	. All Rights Reserved.		

Figure 1 STP information

11.1 STP Information

If you click "Spanning Tree -> STP Information" the top control bar, the STP Information page appears, as shown in figure 2, Priority information is shown in figure 3, and ports information is shown in figure 4.

	2 STP Information G	lobal Configuration	STP Ports	MST Region
Ethernet Status				
60 Link Aggregation	STP Information(MSTP MC	DDE)		
i i chiriggiogatori	Root ID Priority	32768 (0x8000)		
32 Storm Control	Root ID Address	001e.0813.26cc		
III Flow Control	Root ID Hello Time	2 sec		
Port Isolate	Root ID Max Age	20 sec		
O Brabana	Root ID Forward Delay	15 sec		
Port Detect	CIST Root Path Cost	0		
L VLAN	CIST Bridge Priorityt	32768		
B VLAN Classifier	Root ID Priority	32768 (0x8000)		
MAC	Bridge ID Address	001e.0813.26cc		
	Bridge ID Hello Time	2 sec		
留 Spanning Tree 1	Bridge ID Max Age	20 sec		
ka ERPS	Bridge ID Forward Delay	15 sec		
I Mirror	Bridge ID Aging Time	500 sec		

Figure 2 Global information

Parameter usage

ltem	Description
Root ID Priority	Display the priority of the switch which is selected as root
Root ID Address	Display the address of the switch which is selected as root
Root ID Hello Time	Display the hello time interval of the switch which is selected as root
Root ID Max Age	Display the max age of the switch which is selected as root
Root ID Forward Delay	Display the root id forward delay of the switch which is selected as root
CIST Root Path Cost	Display the CIST Root Path Cost
CIST Bridge Priority	Display the CIST Bridge Priority
Bridge ID Priority	Display the bridge ID priority of the switch
Bridge ID Address	Display the bridge ID address of the switch
Bridge ID Hello Time	Display the hello time interval of the switch
Bridge ID Max Age	Display the max age interval of the switch
Bridge ID Forward Delay	Display the forward delay of the switch
Bridge ID Aging Time	Display the of aging time the switch
Edgeport bpdu-filter	Display the enable status of edgeport bpdu-filter
Edgeport bpdu-guard	Display the enable status of edgeport bpdu-guard
Priority Information	Priority

Figure 3 Priority information

• Parameter usage

1

0

32768

ltem			Description						
Instanc	e		Display the Instance Id						
Path Co	st		Display the path cost of the instance						
Priority	/	Display the priority of the instance							
Ports Information	Interface	Port Role	STP Status	Path Cost	Priority.Number	Туре			
					userdes ≢Arther datas				
			Eiguro 4 Dorts inf	ormation					



• Parameter usage

ltem	Description						
Instance	Instance number						
Interface	Interface number for instance operation						
Port Role	Interface status						
STP Status	Display this interface's status on the spanning tree						
Path Cost	The port's internal path cost in this instance						
Priority.Number	The port's internal priority in this instance and port number						
Туре	Link type						

11.2 STP Global

If you click "Spanning Tree -> Global Configuration" in the title bar, the global configuration page appears, as shown in figure 5.

Televent Chater	STP Information 2 Global	Configuration STD Ports MST Region	
CP Emerner status	Good	Shirters instruction	
🕸 Link Aggregation	Global Configuration		
X Storm Control	+ STP	O Enable Disable (Default: Disable)	
11 Flow Control			
Dort Isolate	Advanced Configuration		
Port Detect	BPDU Guard	Enable (Default: Disable)	
님 VLAN	BPDU Filter	O Enable (Default: Disable)	
BB VLAN Classifier	* Working Mode	RSTP	(Default RSTP)
MAC	 Pathcost Standard 	dot1t -	(Default dot1t)
업 Spanning Tree 1			
d₀ ERPS	 Max Age 	20	(6~40, Default 20)
Mirror	= Max Hops	20	(1-40, Default 20)
So Multicast			
A QOS	 Hello Time 	2	
🖄 ACL	Forward Time	15	(4-30, Default 15)

Figure 5 STP global settings

• Parameter usage

ltem	Description
STP	Enable or disable STP on this switch(default: disable)
Nexthop	Set specify nexthop IP address
BPDU Guard	Enable or disable bpdu guard in global
BPDU Filter	Enable or disable bpdu filter in global

Working ModeSpecify types of spanning tree adopted on this switch
STP: select this parameter to set global spanning tree protocol on switch (STP)
RSTP: select this parameter to set global rapid spanning tree protocol on switch (RSTP)
MSTP: select this parameter to set global multiple spanning tree protocol on switch (MSTP)

Item	Description
Pathcost Standard	Choose the standard of path cost calculation. The options are as follow: dot1t, dot1d-1998
Max Age	Max-age ensures that the old information will not be endlessly circled within the network's redundant path, and thus stop the valid transmission of the new information. The value is set by the root bridge to confirm that the spanning tree configuration value of the switch accords with the other devices on the bridge LAN. If the value is timeout, while the switch has not received the BPDU packet from root bridge, the switch starts to send its BPDU to all the other switches to ask for becoming the root bridge. If the switch has the minimal bridge identifier, it will become root bridge. User can set the value from 6-40seconds, the default is 20 seconds
Max Hops	Set the device hops among the devices within spanning tree regions before the BPDU packets are discarded by the switch. The number of hop will be reduced one when each packet passes through the switch until the hop count to zero. At this point, the switch will discard the BPDU packet, and interface information in packet will be time-out. Value ranges from 6 to 40, default is 20
Hello Time	Interval for root bridge's broadcast "hello" message."hello" message is used to detect whether the network topology is normal or not
Forward Time	The setting range is 4-30 seconds (default: 15sec). Each interface on the switch needs to wait double of forward-delay time when the blocked status changes to forwarding status
Instance	Select instance number for the root types needed to configure.
Priority	Bridge priority is used in selecting the root device. The device with the highest priority (the smaller value the higher priority) becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device (note that lower numeric values indicate higher priority) .Default value: 32768; Range: 0~61440; Step Length: 4096

If you want to configure STP global configuration, you can perform the following steps:
(1) Select the configuration items that need to be modified according to the actual needs. The configuration items that do not need to be modified can keep the default value.

Select MSTP in the working mode drop-down box. (2)

After selecting the configuration, you can click "Apply" to complete the configuration. (3)

(4) You can view the configuration in STP information on STP information page.

The operation is shown in figure 6.

* STP	Enable Disable (Default: Disable)	
dvanced Configuration		
* BPDU Guard	Enable Disable (Default: Disable)	
* BPDU Filter:	Enable O Disable (Default: Disable)	
* Working Mode	MSTP	(Default RSTP) 1
* Pathcost Standard	dot1t	▼ (Default dot1t)
* Max Age	20	(640, Default 20)
* Max Hops:	20	(1~40, Default 20)
* Hello Time:	2	(1-10, Default 2)
* Forward Time:	15	(4~30, Default 15)
stance		
* Instance	0	(0-4094)
* Priority:	32768	(0~61440, Default 32768))

Figure 6 Add STP global configuration

11.3 STP Interface

You can configure properties for a specific interface, including port priority, path cost, protection type, and edge port. For ports of the same media type, different priorities or path overhead can be used to indicate the preferred path. Different link types indicate point-to-point connection or shared media connection, while different edge ports indicate that connected devices can support fast forwarding.

If you click "Spanning Tree -> STP Ports" in the title bar, the STP interface page appears, as shown in figure 7.

	CTD Information	Global Configuration	2	CT Region				
C Ethernet Status	STP Information	Giobal Conliguration	STPPOILS	31 Region				
백 Link Aggregation	Ports Status							
3 Storm Control				a. 1 (a).				
Flow Control	Interface Name	Edgeport	Bpdu Guard	Bpdu Filter	Root Guard	Loop Guard	STP	Operation
Dort Isolate	eth-0-1	disable	disable	disable	disable	disable	enable	Edit
Port Detect	eth-0-2	disable	disable	disable	disable	disable	enable	Edit
L VLAN	eth-0-3	disable	disable	disable	disable	disable	enable	Edit
B VLAN Classifier	eth-0-4	disable	disable	disable	disable	disable	enable	Edit
MAC	eth-0-5	disable	disable	disable	disable	disable	enable	Edit
😫 Spanning Tree 1	eth-0-6	disable	disable	disable	disable	disable	enable	Edit
48 ERPS	eth-0-7	disable	disable	disable	disable	disable	enable	Edit
Mirror	eth-0-8	disable	disable	disable	disable	disable	enable	Edit
🖧 Multicast	eth-0-9	disable	disable	disable	disable	disable	enable	Edit
a qos	eth-0-10	disable	disable	disable	disable	disable	enable	Edit
🖸 ACL	eth-0-11	disable	disable	disable	disable	disable	enable	Edit

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved

Figure 7 STP interface

Parameter usage

ltem	Description						
Interface Name	Interface name						
Edgeport	Display this port is enabled edgeport or not						
Bpdu Guard	Display this port is enabled bpdu guard or not						
Bpdu Filter	Display this port is enabled bpdu filter or not						
Root Guard	Display this port is enabled root guard or not						
Loop Guard	Display this port is enabled loop guard or not						
STP	Display this port is enabled STP or not						

If you want to edit the parameters of STP interface "eth-0-1", you can perform the following steps: Click "Edit" corresponding to "eth-0-1" in the interface list, as shown in figure 8, and the configuration page is shown in figure 9.

STP Information	Global Configuration	STP Ports	MST Region					
Ports Status								
Interface Name	Edgeport	Bpdu	ı Guard	Bpdu Filter	Root Guard	Loop Guard	STP	Operation
eth-0-1	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-2	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-3	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-4	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-5	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-6	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-7	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-8	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-9	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-10	disable	disal	ble	disable	disable	disable	enable	Edit
eth-0-11	disable	disal	ble	disable	disable	disable	enable	Edit

Figure 8 STP Settings based on interface operation

Interface	eth-0-1	
• STP	🖲 Enable 💿 Disable	
• Edge port:	enable O Disable	
Bpdu Guard	Enable Disable Disable	
* Bpdu Filter	Enable Disable Disable	
* Root Guard	Enable Disable Disable	
* Loop Guard	 Enable Disable 	
* Instance:	0	(0-4094)
* Priority	128	(0~240,Default 128)
* Path Cost	4	(1-65535)

Figure 9 STP settings based on interface

Parameter usage

ltem	Description
Interface	Current configuration interface
STP	Enable or disable STP on port
Edgeport	Set a port as an edgeport and to enable rapid transitions
Bpdu Guard	Enable or disable the BPDU Guard feature on a port
Bpdu Filter	Enable or disable the BPDU Guard Filter on a port
Root Guard	Enable or disable the Root Guard on a port
Loop Guard	Enable or disable the Loop Guard on a port
Instance	Instance id you want to add this port to.
Priority	The port internal priority in this instance
Path Cost	The port internal path cost in this instance

If you want to configure the STP interface, you can perform the following steps:

- Select the configuration items that need to be modified according to the actual needs. The configuration items that do not need to be modified can keep the default value. (1)
- Use the radio buttons to select "STP", "Edge port" & "Bpdu Guard" as enabled. Click "Submit" button to apply all the changes made.
- (2) (3)

The operation is shown in figure 10.

* STP	Inable Obsable	
* Edge port:	1 💿 Enable 💿 Disable	
* Bpdu Guard	Enable	
* Bpdu Filter	Enable Isable	
* Root Guard	Enable Isable	
* Loop Guard	Enable	
* Instance:	0	(0-4094)
* Priority	128	(0-240,Default 128)
* Path Cost	2000	(1-20000000)
	2 Submit Detail Information Back	

Figure 10 Parameters of editing STP interface

If you want to view the STP interface "eth-0-1" information, you can perform the following steps: (1) You can click the "Detailed Information" button directly on the page of editing STP interface "eth-0-1", the specified interface detail STP configuration information is shown as the figure below.

 Interface
 Role
 State
 Path Cost
 Priority.Port Number
 Type



terface Information	
Dent Chatan	and Pale down
Port Status	port link down
Port Role	port link down
Port Link Type	port link down
Port Priority	128
Port Path Cost	4
Edge Port	disable
Bpdu Guard	disable
Bpdu Filter	disable
Root Guard	disable
Loop Guard	disable
STP Enable	enable
Designated Bridge	000000000000000000000000000000000000000

Figure 11 Display STP Interface Details

• Parameter usage

ltem	Description
Interface	Instance number
Role	Interface status
State	Display this interface's status on the spanning tree: Discarding: port receives STP configuration messages, but does not forward packets Learning: port does not forward packets, and starts to learn MAC address Forwarding: port forwards packets, and continues learning addresses
Path Cost	This interface's internal path cost
Priority.Number	This interface's internal priority and port number
Туре	Link type, point-to-point or shared

• Parameter usage

ltem	Description			
Port Status	Port status in instance			
Port Role	Port role in instance			
Port Link Type	Port Link Type in instance			
Port Priority	Port internal priority in instance			
Port Path Cost	Port internal path cost in instance			
Edgeport	Port in instance is enabled edgeport or not			
Bpdu Guard	Port in instance is enabled bpdu guard or not			
Bpdu Filter	Port in instance is enabled bpdu filter or not			



Item	Description		
Root Guard	Port in instance is enabled root guard or not		
Loop Guard	Port in instance is enabled loop guard or not		
STP Enable	Port in instance is enabled stp or not		
Designated Bridge	Port's designated bridge in instance		

11.4 MST Region

If you click "Spanning Tree -> MST Region" in the title bar, The MST region page appears, as shown in figure 12.

Region			
* Region Name	Please Enter Region Name		
	Apply		
Instance ID			
Add De	lete		
Instance ID		VLAN	
Instance ID0		VLAN 1, 10	

Figure 12 STP Region Information

• Parameter usage

-

Item	Description
Region Name	Specify MST domain name joined by the switch
Instance ID	Display the MST instance ID currently configured on switch.
VLAN	Display VLAN ID mapped to specified MST instance

If you want to add MSTP instance:, you can perform the following steps: If you click "Add", you can add MSTP instance, as shown in figure 13, and then the MSTP instance configuration page appears, as shown in figure 14.

Region Name	122			
0	Apply			
nstance ID				
Add Dele	ste			
Add Dela	te	VLAN		

Figure 13 Add CIST operation

nstance	Please enter	
		(1-4094)
AN list	Please enter	
		example: 2-5,7,9-11

Figure 14 Add CIST

If you want to add CIST, you can perform the following steps:
(1) Select the instance number needed to & in Instance bar, fill in VLAN list.
(2) Click "Apply" button to apply all the changes made.
The operation is shown in figure 15, and the entry of CIST configuration success table is shown in figure 16.

	1	- 1	nstance
(1-4094)	<u></u>	1	
	1		/LAN list
example: 2-579-11	l		

Figure 15 Add CIST configuration

Instance ID		
Add Delete		
Instance ID	VLAN	
0	2, 10, 100, 200, 300, 400	
1	1	

Figure 16 New CIST information

12. ERPS

If you click "Configuration->ERPS" in the top control bar, the ERPS configuration list page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	Configuration	X Maintenance	network	Save	
Ethernet Status	ERPS Configuration	RPS Status					
00 Link Aggregation	CDDC Configuration Information	*!					
IX Storm Control	EKPS Configuration informa	uon					
11 Flow Control	ERPS Mode default			(The configuration wil	I take effect until the next reload)		
Port Isolate	Apply						
Port Detect							
La VLAN	ERPS Configuration Informa	tion					
Cassifier	Add Delete	Refresh					
MAC MAC	🗌 ID 🛛 Name	Pri-\	VLAN Sub-VL	AN Mstp Ins	stance Hello Interval	Fail Interval	Operation
열 Spanning Tree							
I Mirror							
$\mathcal{A}_{h}^{\mathbb{Q}}$ Multicast							
🚇 QOS							
🖄 ACL							
* = = = = =			Copyright ©	2009-2020 FS.COM Inc . A	All Rights Reserved.		

Figure 1 ERPS configuration list

In network planning and practical networking applications, ring network is mostly used to provide high reliability. ERPS technology can improve the availability and durability of Ethernet rings and converge within 50ms of link interruption. This chapter describes the configuration of ERPS.

12.1 ERPS Configuration

With the ERPS configuration feature, you can select the working mode of ERPS, add/remove/modify ERPS domain, and add/remove/modify ERPS ring.

12.1.1 Configure ERPS Mode

If you click "ERPS -> ERPS Configuration" in the title bar, the ERPS mode configuration information page appears, as shown in figure 2, and the ERPS domain configuration information page appears, as shown in figure 4.

Ethernet Status	ERPS Configuration	ERPS Status						
👾 Link Aggregation	2	1						
3 Storm Control	ERPS Configuration	Information						
16 Flow Control	ERPS mode	default			(The configuration	will take effect until the	next reload)	
🕀 Port Isolate		Apply						
Port Detect								
∐ VLAN	ERPS Configuration	Information						
B8 VLAN Classifier	Add	elete Refresh						
🖳 MAC	D ID	Name	Pri-Vlan	Sub-Vlan	Mstp Instance	Hello interval	Fail interval	Operate
😄 Spanning Tree	0 1	fs	100	200	0	40	400	Edit
≪ ERPS 1	2	ух	300	400	00	30	300	Edit

Figure 2 ERPS mode configuration information

Parameter usage

ltem	Description
ERPS mode	Display the working mode of ERPS, which supports RRPP protocol compatibility

If you want to modify the working mode of ERPS, please select the working mode from the "ERPS mode" dropdown box, and then click

the "Apply" button, the operation is shown in figure 3.

ERPS Configurat	ion Information			
ERPS mode	default	 (The configuration will take effect until 	l the next reload) 1	
	default RRPD Approv			

Figure 3 Select the working mode of ERPS

12.1.2 Add the ERPS Domain

] ID	Name	Pri-Vlan	Sub-Vlan	Mstp Instance	Hello interval	Fail interval	Operat

Figure 4 ERPS domain configuration information

• Parameter usage

ltem	Description
ID	Display the ERPS domain ID
Name	Display the ERPS domain name
Pri-Vlan	Display the primary control VLAN for ERPS
Sub-Vlan	Display a sub control VLAN for ERPS
Mstp Instance	Display an MSTP instance
Hello interval	Display the Hello message delivery period
Fail interval	Display the Fail message delivery period
Operate	Display that ERPS domain table entries can be edited

If you click "Add" button, you can add an ERPS domain, the operation is shown in figure 5, and then the ERPS domain configuration page appears, as shown in figure 6.



Figure 5 Add ERPS domain operation

ERPS Domain Con	figuration	
Domain ID	Please enter the field ID	
Domain Name	Please enter the domain name	("Domain name character should be "0-9A-Za-z" the first character should be a-z or A-Z and the last character should be 0-9 or a-z or A-Z")
Primary VLAN	Please enter the primary VLAN	(2-4094)
Sub VLAN	Please enter the subvlan	(2-4094)
Mstp Instance	Please enter an MSTP instance	(0-4094)
Hello Interval	Please enter Hello cycle	(1~150, uint 100ms)
Fail Interval	Please enter the Fail cycle	(3~450, uint 100ms)
Ring List	· · · · · · · · · · · · · · · · · · ·	🕞 New 🖉 Modify 🔟 Delete
	Submit Back	

Figure 6 Add ERPS domain

Parameter usage

ltem	Description
ID	Set the ERPS domain ID
Name	Set the ERPS domain name
Pri-Vlan	Set the primary control VLAN for ERPS
Sub-Vlan	Set a sub control VLAN for ERPS
Mstp Instance	Set an MSTP instance
Hello interval	Set the Hello message delivery period
Fail interval	Set the Fail message delivery period
Ring List	Display ERPS ring list information

If you want to add an ERPS domain, you can follow the following steps:

- (1) Enter an ERPS domain ID in the "ID" textbox.
- (2) Enter an ERPS domain name in the "Name" textbox.
- (3) Enter an ERPS primary control VLAN in the "Pri-Vlan" textbox.
- (4) Enter an ERPS sub control VLAN in the "Sub-Vlan" textbox.
- (5) Enter an MSTP instance in the "Mstp Instance" textbox.
- (6) Enter the Hello message delivery period in the "Hello interval" textbox, but the parameters are optional, and if not configured, the default value is 1 second.
- (7) Enter the Fail message delivery period in the "Fail interval" textbox, but the parameters are optional, and if not configured, the default value is 3 second.
- (8) Click the "Submit" button.
- The operation is shown in figure 7, the ERPS domain configured the successful table entry information is shown in figure 8.

ERPS	Domain	Configuration	

Please enter the field ID	(1-255)	1
Please enter the domain name	("Domain n a-z or A-Z a	name character should be "0-9A-Za-z" the first character should be and the last character should be 0-9 or a-z or A-Z")
Please enter the primary VLAN	(2-4094)	3
Please enter the subvlan	(2-4094)	4
Please enter an MSTP instance	(0-4094)	5
Please enter Hello cycle) (1~150, uin	at 100ms) 6
Please enter the Fail cycle	(3~450, uin	it 100ms) 7
	[↓ N	ew 🖉 Modify 🗑 Delete
	Please enter the field ID Please enter the domain name Please enter the primary VLAN Please enter the subvlan Please enter an MSTP instance Please enter Hello cycle Please enter the Fail cycle	Please enter the field ID (1-255) Please enter the domain name (*Domain name a-z or A-Z-z) Please enter the primary VLAN (2-4094) Please enter the subvlan (2-4094) Please enter an MSTP instance (0-4094) Please enter Hello cycle (1-150, uir Please enter the Fail cycle (3-450, uir



ERPS Domain Con	figuration	
Domain ID	1	
		("Domain name character should be "0.04.76.7" the first character should be
Domain Name	fs	a-z or A-Z and the last character should be 0-9 or a-z or A-Z*)
Primary VLAN	100	(2-4094)
Sub VLAN	200	(2-4094)
Mstp Instance	0	(0-4094)
Hello Interval	40	(1-150, uint 100ms)
Fail Interval	400	(3~450, uint 100ms)
Ring List	v	🕞 New 🖉 Modify 🗑 Delete
	Submit Back	
	Figure 8 New ERPS	domain information

12.1.3 Add the ERPS Ring

In the ERPS domain configuration page, if you click "New" button, you can add an ERPS ring, the operation is shown in figure 9, and then the ERPS ring configuration page appears, as shown in figure 10.

Domain ID		
	1	
Domain Name	fs	("Domain name character should be '0-9A-Za-z-," the first character should be a-z or A-Z and the last character should be 0.9 or a-z or A-Z")
Primary VLAN	100	(2-4094)
Sub VLAN	200	(2-4094)
Mstp Instance	0	(5-4094)
Hello Interval	40	
Fail Interval	400	(3~450, uint 100ms)
Ring List		Da New 🖉 Modify 😇 Delete



RPS Ring Configuration]			
Ring ID	Please ent	ter the field II	2	(1-255
Ring Level	Primary	Sub 🔘		
Ring Edge Mode	None	🔘 Edge	Assistant-edge	
Ring Mode	O Master	🔘 Transit	◎ Vpls	
Ring Primary Interface				
Ring secondary Interface				
Ring Vpls Interface				
Ring Edge Interface			×	
Ring Common Interface			•	
Ring Srpt	Enable	Oisable		
Ring Status	🔘 Enable	 Disable 		
	Submit	Bac	k	

Figure 10 Add ERPS ring

Parameter usage

ltem	Description
Ring ID	Specifies the ERPS ring ID
Ring Level	Specifies that the ERPS ring is the primary ring or sub ring
Ring Edge Mode	Specifies the edge mode of the ERPS ring
Ring Mode	Specifies the node mode for the ERPS ring
Ring Primary Interface	Select the primary interface of the ERPS ring
Ring secondary Interface	Select the secondary interface of the ERPS ring
Ring Vpls Interface	Select the VPLS interface for the ERPS ring
Ring Edge Interface	Select the edge interface of the ERPS ring
Ring Common Interface	Select the common interface of the ERPS ring
Ring Srpt	Enable or disable SRPT message delivery
Ring Status	Enable or disable the ERPS ring

If you want to add a primary ring primary node, you can follow the following steps:

- Enter an ERPS ring ID in the "Ring ID" textbox. (1)
- Select the ERPS ring is the primary ring in the "Ring Level" radio buttons. (2)
- Select the edge mode of the ERPS ring to be none in the "Ring Edge Mode" radio buttons. Select the node mode of the ERPS ring as master in the "Ring Mode" radio buttons. (3)
- (4)
- (5) Select the primary interface of the ERPS in the "Ring Primary Interface" dropdown box.
- Select the secondary interface of the ERPS in the "Ring secondary Interface" dropdown box. (6)
- (7) Select the Vpls interface of the ERPS in the "Ring Vpls Interface" dropdown box.
- Enable ERPS ring function in the "Ring Status" radio buttons. (8)
- Click the "Submit" button. (9)

The operation is shown in figure 11, the ERPS ring configured the successful table entry information is shown in figure 12.

* Ring ID	1	(1-255) 1
Ring Level	Primary Sub	
Ring Edge Mode	None	
Ring Mode	⊛ Master ⊚ Transit ⊚ Vpls 4	
Ring Primary Interface	eth-0-15	• 5
Ring secondary Interface	eth-0-16	• 6
Ring Vpls Interface	eth-0-17	, 7
Ring Edge Interface		v
ERing Common Interface		Ψ.
Ring Srpt	Enable Disable	
Ring Status	Enable Disable B	
	Submit Back 9	

Figure 11 Add ERPS ring configuration

ERPS Ring Configuration	n	
* Ring ID	1	
Ring Level	Primary Sub	
Ring Edge Mode	None Edge Assistant-edge	
Ring Mode	Master	
Ring Primary Interface	eth-0-15	×
Ring secondary Interface	e eth-0-16	v
Ring Vpls Interface	eth-0-17	×
Ring Edge Interface		×
ERing Common Interface	e	v
Ring Srpt	Enable Disable Disable	
Ring Status	Enable Disable Disable	



12.1.4 Modify the ERPS Ring

In the ERPS domain configuration page, if you click "Modify" button, you can modify an ERPS ring configuration, the operation is shown in figure 13, and then the ERPS ring configuration page appears, as shown in figure 14.

EC
ГЭ

ERPS Domain Conf	liguration	
Domain ID	i	
Domain Name	fs	("Domain name character should be "0-00-Ze- z " the first character should be a-t or A-Z and the last character should be 0-9 or a-c or A-Z")
Primary VLAN	100	(2-4034)
Sub VLAN	200	(2-4094)
Mstp Instance	0	(0-4014)
Hello Interval	40	
Fail Interval	400	(3-450, uint 100ms)
Ring List	1(primary) *	De New 2 Modify 😇 Delete
	Submit Back	

Figure 13 Modify ERPS ring operation

* Ring ID	1	(1-255)
Ring Level	Primary Sub	
Ring Edge Mode	None Edge Assistant-edge	
Ring Mode	Master O Transit Vpls	
Ring Primary Interface	eth-0-15 v	
Ring secondary Interface	eth-0-16 v	
Ring Vpls Interface	eth-0-17 v	
Ring Edge Interface	· · ·	
ERing Common Interface	v	
Ring Srpt	enable Disable	
Ring Status	Enable Disable Disable	
	Submit Back	

Figure 14 ERPS ring configuration

Parameter usage

ltem	Description
Ring ID	Display the ERPS ring ID
Ring Level	Display the level of the ERPS ring
Ring Edge Mode	Display the edge mode of the ERPS ring
Ring Mode	Display the node mode for the ERPS ring
Ring Primary Interface	Display the primary interface of the ERPS ring
Ring secondary Interface	Display the secondary interface of the ERPS ring
Ring Vpls Interface	Display the VPLS interface for the ERPS ring
Ring Edge Interface	Display the edge interface of the ERPS ring
ltem	Description
Ring Common Interface	Display the common interface of the ERPS ring
Ring Srpt	Display the status of ERPS ring SRPT message delivery
Ring Status	Display the status of ERPS ring function

By selecting enable or disable the ERPS ring feature in the "Ring Status" radio buttons, and then click "Submit" button, you can modify the configuration of the ERPS ring, the operation is shown in figure 15.

≮ Ring ID	1	(1-255)
Ring Level	e Primary Sub	
Ring Edge Mode	None Edge Assistant-edge	
Ring Mode	Master O Transit Vpls	
Ring Primary Interface	eth-0-15 v	
Ring secondary Interface	eth-0-16 *	
Ring Vpls Interface	eth-0-17 •	
Ring Edge Interface	т	
ERing Common Interface		
Ring Srpt	Enable Disable	
Ring Status 1	enable Oisable	
2	Submit Back	



12.1.5 Remove the ERPS Ring

In the ERPS domain configuration page, if you "Delete" button, you can delete an ERPS ring, the operation is shown in figure 16, and then the delete ERPS ring successful page appears, as shown in figure 17.

ERPS Domain Cont	figuration	
Domain ID	1	
Domain Name	h	("Domain name character should be "0-40-Zu-zu-" the first character should be $u \in \sigma A - Z$ and the last character should be $0.9 \sigma \sigma s - \sigma a - Z^{-1}$
Primary VLAN	100	(2-4014)
Sub VLAN	200	(2-4094)
Mstp Instance	0	(0-4014)
Hello Interval	40	
Fail Interval	400	(3-450, ulet 100ms)
Ring List	1(primary) T	🕞 New 🖉 Modify 🔁 Delete
	Submit Back	
		Figure 16 Delete ERPS ring operation
ERPS Domain Conf	Iguration	Figure 16 Delete ERPS ring operation
ERPS Domain Conf Domain ID	Iguration	Figure 16 Delete ERPS ring operation
ERPS Domain Cont Domain ID Domain Name	liguration 1 fs	Figure 16 Delete ERPS ring operation 0:253 CDomain name character shead he '0-30-25 ' the first character shead he is rear of 2 and the last character shead he is 0 are a c a 2.2)
ERPS Domain Conf Domain ID Domain Name Primary VLAN	figuration 1 fs 100	Figure 16 Delete ERPS ring operation (+25) (*25) (*20min name character should be *2-84-22-2; the first character should be are a A2 and the last character should be 9-9 or a c or A.2; (*-694)
ERPS Domain Conf Domain ID Domain Name Primary VLAN Sub VLAN	Iguration 1 fs 100 200	Figure 16 Delete ERPS ring operation (1-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25) (2-25)
ERPS Domain Conf Domain ID Domain Name Primary VLAN Sub VLAN Mstp Instance	fguration 1 fs 1 200 0	Figure 16 Delete ERPS ring operation (1-25) (2-25) (2-25) (2-465) (2-465) (2-465) (2-465) (2-465) (2-465)
ERPS Domain Conf Domain ID Domain Name Primary VLAN Sub VLAN Mstp Instance Hello Interval	Iguration 1 fs 100 200 0 40	Figure 16 Delete ERPS ring operation (+25) (*25) (*26%) (*46\%) (*46\%) (*
ERPS Domain Conf Domain ID Domain Name Primary VLAN Sub VLAN Mstp Instance Hello Interval Fail Interval	Iguration 1 5 5 100 200 0 40 40	Figure 16 Delete ERPS ring operation (1-25) (2-25)
ERPS Domain Conf Domain ID Domain Name Primary VLAN Sub VLAN Mstp Instance Hello Interval Fall Interval Ring List	Iguration 1 5 5 6 40 400	Figure 16 Delete ERPS ring operation



12.1.6 Modify the ERPS Domain

In the ERPS domain information display page, if you click "Edit" button, you can modify an ERPS domain configuration, the operation is shown in figure 18, and then the ERPS domain configuration page appears, as shown in figure 19.

~							
PS Configurati	on Information						
ERPS mode	default			 (The configuration) 	will take effect until the	next reload)	
	Apply						
PS Configuration	Apply on Information Delete Refresh						
PS Configuration	Apply on Information Delete Refresh Name	Pri-Vlan	Sub-Vlan	Mstp Instance	Hello interval	Fail interval	Opera

Figure 18 Modify ERPS domain configuration operation

ERPS Domain Conf	iguration	
Domain ID	1	
Domain Name	fs	("Domain name character should be "0-9A-Zb-z-," the first character should be a-z or A-Z and the last character should be 0-9 or a-z or A-Z")
Primary VLAN	100	(2-409-4)
Sub VLAN	200	(2-4094)
Mstp Instance	0	(0-4094)
Hello Interval	40	
Fail Interval	400	(3-450, uint 100ms)
Ring List		D. New & Modify 🔒 Delete
	Submit Back	

Figure 19 ERPS domain configuration

• Parameter usage

ltem	Description
Domain ID	Display the ERPS domain ID
Domain Name	Display the ERPS domain name
Primary Vlan	Set the primary control VLAN for ERPS
Sub Vlan	Set a sub control VLAN for ERPS
Mstp Instance	Set an MSTP instance
Hello interval	Set the Hello message delivery period
Fail interval	Set the Fail message delivery period
Ring List	Display ERPS ring list information

If you want to modify the configuration of the ERPS domain, you can follow the following steps:

- (1) Enter an ERPS primary control VLAN in the "Pri-Vlan" textbox.
- (2) Enter an ERPS sub control VLAN in the "Sub-Vlan" textbox.
- (3) Enter an MSTP instance in the "Mstp Instance" textbox.
- (4) Enter the Hello message delivery period in the "Hello interval" textbox, but the parameters are optional, and if not configured, the default value is 1 second.
- (5) Enter the Fail message delivery period in the "Fail interval" textbox, but the parameters are optional, and if not configured, the default value is 3 second.
- (6) Click the "Submit" button.

The operation is shown in figure 20, the table entry information that ERPS domain successfully modified is shown in figure 21.

ERPS Domain Cor	nfiguration	
Domain ID	1	
Domain Name	fs	("Domain name character should be "9-9A-Za- \pm " the first character should be a.s. or A-Z and the last character should be 0-9 or a.s. or A-Z")
Primary VLAN	300	2-4094) 1
Sub VLAN	400	(2-4094) 2
Mstp Instance	0	(2-4094) 3
Hello Interval	30	(1-150, ulrd 100mm) 4
Fail Interval	300	(1-450, ulid 100ms) 5
Ring List	· · · · · · · · · · · · · · · · · · ·	🕞 New 🖉 Modify 🗇 Delete
6	Submit Back	

Figure 20 Modify ERPS domain configuration

ERPS Domain Conf	iguration	
Domain ID	1	
Domain Name	fs	("Domain name character should be "0-9A-Za- $z_{}$ " the first character should be a vz or A-Z and the last character should be 0-9 or a z or A-Z)
Primary VLAN	300	(2-409-0)
Sub VLAN	400	(2-403-4)
Mstp Instance	0	(0-4034)
Hello Interval	30	(1-150, wint 100ms)
Fail Interval	300	(3-450, uint 100m)
Ring List		🕞 New & Modify 🖨 Delete
	Submit Back	

Figure 21 ERPS domain configuration information

12.1.7 Remove the ERPS Domain

If you want to delete the specified ERPS domain, you can follow the following steps:

- (1) Select this specified ERPS domain which you want to delete.
- (2) Click "Delete" button.
- (3) It will appear tips page to note you to confirm the operation, as shown in figure 22, if you click "Confirm" button, it will delete the ERPS domain, the table entry that ERPS domain successfully deleted is shown in figure 23; if you click "Cancel" button, you will cancel the delete operation.

RPS Configurati	ion Information						
ERPS mode	default				e	rt until the next reload)	
	Apply	Ti	ps		×		
			Are you sure to dele	te the selected ERPS			
Add Configurati	Delete Refresh		configuration data?				
D ID	2 Name	Pri-Vlan	Confirm	Cancel	٦t	erval Fail interval	Operate
1	fs	300	400 Figure 22 Delet	o te ERPS doma	30	300	Edit
I 1 ERPS Configuration	fs n ERPS Status	300	400 Figure 22 Delet	o te ERPS doma	30	300	Edit
I I ERPS Configuration	fs n ERPS Status on Information	300	400 Figure 22 Delet	0 te ERPS doma	30	300	Edit
ERPS Configuration	fs n ERPS Status on Information default	300	400 Figure 22 Delet	o te ERPS doma	30 in	300 rt until the next reload)	Edit
I ERPS Configuration RPS Configuration ERPS mode.	fs n ERPS Status on Information default Apply	300	400 Figure 22 Delet	o te ERPS doma	30 in	300 :t until the next reload)	Edit
I I I I RPS Configuration RPS Configuration RPS mode. RPS Configuration	fs n ERPS Status on Information default Apply on Information	300	400 Figure 22 Delet	o te ERPS doma	30 in	300 .t until the next reload)	Edit
Provide a configuration Provi	fs n ERPS Status on Information default Apply on Information Delete Refresh	300	400 Figure 22 Delet	o te ERPS doma	30 in	300 ct until the next reload)	Edit

Figure 23 ERPS domain configuration information

12.1.8 Refresh the ERPS Domain

if you want to refresh the ERPS domain configuration information, you can click "Refresh" button. The operation is shown in figure 24.

ERPS Co	onfiguration	ERPS Status						
ERPS Co	onfiguration Ir	formation						
ERPS	mode	default			(The configuration	will take effect until the r	next reload)	
		Apply						
FRPS Co	onfiguration Ir	formation						
	dd Dele	te Refresh						
	ID	Name	Pri-Vlan	Sub-Vlan	Mstp Instance	Hello interval	Fail interval	Operate
	1	fs	100	200	0	40	400	Edit
	2	VX	300	400	00	30	300	Edit

Figure 24 Refresh the ERPS domain configuration information

12.2 ERPS Status

This section describes the state information and statistics of the ERPS domain.

12.2.1 ERPS Status Information

If you click "ERPS -> ERPS Status" in the title bar, the ERPS status information page appears, as shown in figure 25.

🐨 Ethernet Status	ERPS Configuration ERPS Status 2
🔅 Link Aggregation	ERPS Status Information
3% Storm Control	
11 Flow Control	ERPS Domain 1 View
Port Isolate	Clear Statistics
Port Detect	Statistics
∐ VLAN	
B VLAN Classifier	
MAC	
열 Spanning Tree	
& ERPS 1	

Figure 25 ERPS status information

• Parameter usage

ltem	Description
ERPS Domain	Display the domain ID information for the ERPS domain

If you want to view the status of different ERPS domains, please select the ERPS domain ID in the "ERPS Domain" dropdown box, and then click the "View" button, the operation is shown in figure 26, the state information for the ERPS domain is shown in figure 27.

RPS Configuration	ERPS Status		
'S Status Information	n1	2	
RPS Domain		View	
Clear Statistics ²			
Statistics			

Figure 26 View ERPS status operation

ERPS Configuration	ion ERPS Status		
ERPS Status Info	ormation		
ERPS Domain	1	v View	
Clear Statis	stics		
Statistics			
ERPS ring ID: 1			
ERPS ring level	l: primary		
ERPS ring 1 no	ide mode: transit		
ERPS ring 1 no	de state: link down		
ERPS ring 1 pri	imary interface name: eth-0-15 state:unblock		
Sent:			
total packets:0			

Figure 27 ERPS status information

If you want to clear the ERPS domain's statistics, please click the "Clear Statistics" button, the operation is shown in figure 28.

ERPS Configuration	ERPS Status		
ERPS Status Informatio	on		
ERPS Domain 1		View	
Clear Statistics]		
Statistics			
ERPS ring ID: 1			
ERPS ring level: prima	ſŷ		
ERPS ring 1 node mod	de: transit		
ERPS ring 1 node state	e: link down		
ERPS ring 1 primary in	nterface name: eth-0-15 state:unblock		
Sent:			



13. Mirror

If you click "Configuration -> Mirror" in the top control bar, the mirror configuration list page appears, as shown in figure 1.

Global Co

FS S5800-8TF12S

Ethernet Status



🕸 Link Aggregation										
31 Storm Control	Mirror Configuration									
Flow Control	Add	ete Refresh								
Port Isolate	Session ID	Туре	Source Port TX	Source Port RX	Source Port Both	Source VLAN TX	Source VLAN RX	Source VLAN Both	Destination	Operation
Port Detect										
L VLAN										
VLAN Classifier										
MAC										
Spanning Tree										
C ERPS										
Mirror 2					No Data~					
% Multicast										
QOS										
Z ACL										
				Copyright (© 2009-2020 FS.COM II	ic . All Rights Reserved	£30			

Figure 1 Mirror list

This section mainly describes how to configure and view Mirror.

13.1 Mirror Configuration

If you click "Mirror -> Mirror Configuration" in the title bar, the mirror configuration information page appears, as shown in figure 2.

🕑 Ethernet Status	Mirror Configuration 2 Global Configuration Escape MAC for Remote Mirror	
帥 Link Aggregation		
31 Storm Control	Mirror Configuration	
Flow Control	Add Delete Refresh	
🖻 Port Isolate	Session ID Type Source Port TX Source Port RX Source Port Both Source VLAN TX Source VLAN RX Source VLAN Both Destination Operation	m
Port Detect		
L VLAN		
B VLAN Classifier		
MAC		
留 Spanning Tree		
4 ERPS		
I Mirror	No Data-	



• Parameter usage

ltem	Description
Session ID	Display the session ID of mirror
Туре	Display the destination type of mirror, including local/Remote port Mirroring
Source PORT TX	Display mirroring of the receiving direction of a port

ltem	Description
Source PORT RX	Display mirroring of the sending direction of a port
Source PORT BOTH	Display mirroring of the sending and receiving direction of a port
Source VLAN TX	Display mirroring of the receiving direction of a VLAN
Source VLAN RX	Display mirroring of the sending direction of a VLAN
Source VLAN BOTH	Display mirroring of the sending and receiving direction of a VLAN
Destination	Display mirrored destination port
Operation	Display that mirror configuration table entries can be edited

13.1.1 Add Mirror Sessions

If you click "Add" in the mirror configuration list, you can add a mirror session, the operation is shown in figure 3. then mirror session settings page appears, as shown in figure 4.

or Configuration		
Add Delete Refresh		
] Session ID Type	Source Port TX Source Port RX Source Port Both Source VLAN TX Source VLAN RX Source VLAN Bo	th Destination Operat
	Figure 3 Add mirror sessions operation	
Airror Session Settings		
Session ID	1	
Source Port	•	
Direction		
Source VLAN		(1-4094)
Direction	~	
Destination Type	remote 💌	
Destination VLAN) (2~4094)
Destination Dest	eth-0-1	

Figure 4 Mirror sessions settings list

Parameter usage

Item	Description
Session ID	Display the session ID of mirror
Source Port	Display the source port of mirror
Direction	Display the direction of source port
Source VLAN	Display the source vlan of mirror
Direction	Display the direction of source vlan
Direction Type	Display the type of the mirror target (remote or local)
Direction VLAN	Display mirroring target VLAN (remote support only)
Direction port	Display the destination port of mirror

If you want to add a mirror session, you can follow the following steps:

- (1) Select a session ID.
- (2) Select a source port for configuration mirroring.
- (3) Select the direction of source port.
- (4) Select the destination type of mirror.
- (5) Enter the destination VLAN of mirror.
- (6) Select the destination port of mirror.
- (7) Click the "Apply" button to add a mirror session.

NOTE:

- (1) The items with the asterisk symbol "*" are ones where you must enter values.
- (2) A mirroring session is a collection of mirroring sources and a mirroring purpose, for a mirroring session to work, you need to configure a mirroring destination and at least one mirroring source.

The operation is shown in figure 5, add a mirror session configuration success table entry is shown in figure 6.



Figure 5 Add mirror session configuration

Figure 6 New mirror session information

13.1.2 Modify Mirror

You can click the "Edit" button in the rightmost operation bar to modify the mirror information of the session, this operation is shown in figure 7, and then port mirror configuration page appears, as shown in figure 8.

virror Configuration									
Add Dele	Refresh								
Session ID	Туре	Source Port TX	Source Port RX	Source Port Both	Source VLAN TX	Source VLAN RX	Source VLAN Both	Destination	Operation
1	Remote	N/A	eth-0-7	N/A	N/A	N/A	N/A	eth-0-11 (vlan 2)	Edit
			Figure 7 E	dit mirror se	ssion opera	tion			
Mirror Session	Settings								
Back									
Session ID		1							
Source Info									
Port receive o	nly	eth-0-7							
Port trasmit o	nly	N/A							
Port both dire	ction	N/A							
VLAN receive	only	N/A							
VLAN trasmit	only	N/A							
VLAN both di	rection	N/A							
Mirror Session II	nformation								
Source Config	uration								
Source Port		eth-0-1				-			
Direction		both				Ŧ			
		Add	Delete						

Figure 8 Port mirror configuration page

• Parameter usage

ltem	Description
Port receive only	Display port only receive packets
Port transmit only	Display port only transmit packets
Port both direction	Display port both transmit and receive packets
VLAN receive only	Display VLAN only receive packets
VLAN transmit only	Display VLAN only transmit packets
VLAN both direction	Display VLAN both transmit and receive packets

If you want to modify the specified mirror, such as add a source port to receive and send packets in a mirroring session, and then modify the destination port in this mirroring session, you can follow the following steps:

(1) Select a new source port.

(2) Select the direction of receiving and sending packets.

(3) Click the "Add" button to add a source port to the mirroring session.

(4) Select a new destination port.

(5) Click the "Apply" button to modify the destination port in this mirroring session.

NOTE: The items with the asterisk symbol "*" are ones where you must enter values.

The operation is shown in figure 9, modify specified mirror success table entry is shown in figure 10 and figure 11.

ource Port	eth-0-8	- 1
Direction	both	- 2
	3 Add Delete	
Source VLAN		(1~4094)
Direction	both	*
	Add Delete	
Destination Configuration		
Destination Type	Remote	v
Destination VLAN	2	(2-4094)
Destination Port	eth-0-20	- 4

Figure 9 Edit mirror session operation

Mirror Session Settings

Back				
Session ID	1			
Source Info				
Port receive only	eth-0-7			
Port trasmit only	N/A			
Port both direction	eth-0-8			
VLAN receive only	N/A			
VLAN trasmit only	N/A			
VLAN both direction	N/A			

Figure 10 Modified mirroring session information

Mirror Configuration									
Add Dele	Refresh								
Session ID	Туре	Source Port TX	Source Port RX	Source Port Both	Source VLAN TX	Source VLAN RX	Source VLAN Both	Destination	Operation
0 1	Remote	N/A	eth-0-7	eth-0-8	N/A	N/A	N/A	eth-0-20 (vlan 2)	Edit



13.1.3 Delete Mirror

If you want to delete the specified mirror, you can follow the following steps:

- (1) Choose the check box in the left-hand column of the specified mirror.
- (2) Click "Delete" button.
- (3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button, it will delete this mirror; if you click "cancel" button, you will cancel delete this mirror operation, as shown in figure 12.

M	Add Delete	2 Refresh								
	Session ID	Туре	Source Port TX	Source Port RX	Source Port Both	Source VLAN TX	Source VLAN RX	Source VLAN Both	Destination	Operation
1	1	Remote	N/A	eth-0-7	eth-0-8	N/A	N/A	N/A	eth-0-20	Edit
									(vlan 2)	

Figure 12 Delete mirror operation

Delete a mirror configuration success table entry is shown in figure 13.

Mirror Configuration	Global Co	nfiguration Escap	e MAC for Remote M	irror					
Mirror Configuratio	n elete Refresh								
Session ID	Туре	Source Port TX	Source Port RX	Source Port Both	Source VLAN TX	Source VLAN RX	Source VLAN Both	Destination	Operation

Figure 13 Delete mirror information

13.2 Global Configuration

If you click "Mirror -> Global configuration" in the title bar, the global configuration information page appears, as shown in figure 14.



FS <u>S5800-8TF12S</u>		Monitor	Configuration	X Maintenance	Network
🖱 Ethernet Status	Mirror Configuration 2 Global G	Configuration Escape MA	C for Remote Mirror		
Storm Control	Global Configuration * Dest port forwarding enable	O Enable O Disable (Default	: Disable)		
Flow Control Flow Isolate		Apply			
Port Detect					
VLAN Classifier					
MAC Spanning Tree					
Gerps					
La Multicast					
🗱 QOS					
	Figu	ure 14 Global configu	iration list		

Parameter usage

ltem	Description
Dest port forwarding enable	Display whether the normal forwarding function of dest port is enabled globally

13.2.1 Configure Destination Port Forwarding Function

If you want to configure destination port forwarding function, such as enable destination port forwarding function, you can click the "Enable" button and then click the "Apply" button. The operation is shown in figure 15.

Mirror Configuration	Global Configuration	Escape MAC for Remote Mirror
Global Configuration * Dest port forwarding enable	e 1 OEnable () Disable (Default: Disable)
	2 Apply	



13.3 Escape MAC for Remote Mirror

If you click "Mirror -> Escape MAC for Remote Mirror" in the title bar, the escape MAC for remote mirror page appears, as shown in figure 16.

Ethernet Status	Mirror Configuration	Global Configuration 2	Escape MAC for Remote Mirror	
< Link Aggregation			~	
X Storm Control	Escape MAC for Remot	e Mirror		
15 Flow Control	Mac Address	i i		
Dort Isolate	Mask	× ×		
Port Detect	Add Delete	Refresh		
∐ VLAN				
B8 VLAN Classifier	Mac Address		Mask	
mac Mac				
躍 Spanning Tree				
🐇 ERPS				
Mirror 1				
暑 Multicast				
QOS				
ACL				
				No Data~
			C	Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Figure 16 Escape MAC for remote mirror list

Parameter usage

ltem	Description
Mac Address	Displays the Escape MAC address of the remote mirror

13.3.1 Add Escape MAC for Remote Mirror

If you want to add escape MAC for remote mirror, you can follow the following steps:

- (1) Enter a valid MAC address.
- (2) Enter a valid Mask address.
- (3) Click the "Add" button to add escape MAC for remote mirror.
- The operation is shown in figure 17, add escape MAC for remote mirror success table entry is shown in figure 18.

Mirror Configuration	Global Configuration	Escape MAC for Remote Mirror	
Escape MAC for Remot	e Mirror		
Mac Address 1	aeb6 , d0c9 , 5987	(0.0.0)	
Mask 2	ffff . ffff . ffff	(0.0.0)]
Add Delete	Refresh		

Figure 17 Add escape MAC for remote mirror operation

irror Configuration	Global Configuration	Escape MAC for Remote Mirror	
cape MAC for Remote	Mirror		
Mac Address	a a		
Mask	a a		
Mask Delete	Refresh		
Mac Address		Mask	
aeb6.d0c9.5987		ffff.ffff.ffff	

Figure 18 New escape MAC for remote mirror

13.3.2 Delete Escape MAC for Remote Mirror

If you want to delete the specified escape MAC for remote mirror, you can follow the following steps:

- (1) Choose the check box in the left-hand column of the specified escape MAC for remote mirror.
- (2) Click "Delete" button.
- (3) It will appear tips page to note you to confirm the operation, if you click "Confirm" button, it will delete this escape MAC for remote mirror; if you click "cancel" button, you will cancel delete this escape MAC for remote operation, as shown in figure 19.

Mirror Configuration	Global Configuration	Escape MAC for Remote Mirror		
scape MAC for Remot	e Mirror			
Mac Address				
Mask	t: t.			
2				
Add	Refresh	ti	DS	×
Mac Address		Mask		
1 🛃 aeb6.d0c9.5987		ffff.ffff.ff		1002
hormon constructions			The you sure to delete selected in	arte.
			3 Confirm Cancel	

Figure 19 Delete escape MAC for remote mirror operation

Delete escape MAC for remote mirror success table entry is shown in figure 20.
Escape MAC for Re	mote Mirror		
Mac Address	· ·		
Mask			
Add	Refresh		
Mac Address		Mask	



Figure 20 Delete escape MAC for remote mirror

14. Multicast

If you click "Network ->IP Routing" in the top control bar, the multicast configuration list page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	1 Configuration	Maintenance	network	
Ethernet Status	IGMP Snooping IGMP S	incoping Information				
00 Link Aggregation	ICMD Secondary Clobal					
🐹 Storm Control	IGMP Shooping Global					
Elow Control	 IGMP Snooping 	Enable		Ŧ		
Port Isolate	Max Member Number	1024			(1-8192, Default 8192)	
Port Detect	 TCN Querier Count 	2				
La VLAN						
BB VLAN Classifier	 TCN Querier Interval 	10			(1-255, Default 10)	
MAC		Apply				
열 Spanning Tree						
48 ERPS	IGMP Snooping Vlan					
I Mirror	• Vlan Mode	All Vlan		Ŧ		
🔏 Multicast 2	* Vlan ID	1			(1-4094)	
🚇 QOS	IGMP Spooning	Enable				
🖸 ACL	- tottir shooping	Linable				
	Discard Holonwo	Dirohla		-		
			Copyright	© 2009-2020 FS.COM I	nc . All Rights Reserved.	

Figure 1 Multicast configuration list

This chapter describes multicast configuration function and viewing multicast information of the device.

14.1 IGMP Snooping

The multicast configuration capabilities include IGMP snooping global configuration and IGMP snooping VLAN configuration.

14.1.1 IGMP Snooping Global Configuration

If you click "Multicast-> IGMP Snooping" in the title bar, the IGMP snooping global configuration page appears, as shown in figure 2.

	IGMP Snooping IGMP Snoo	ping Information	
Ethernet Status	2		
👾 Link Aggregation	IGMP Snooping Global		
🕱 Storm Control	 IGMP Snooping 	Disable	
1 Flow Control	 Max Member Number 	200	(1-2048, Default 2048)
🕀 Port Isolate	TCN Oursine Count	Γ.	
D Port Detect	CN Quener Count	3	
L VLAN	 TCN Querier Interval 	100	(1-255, Default 10)
B VLAN Classifier		Apply	
MAC			
😫 Spanning Tree	IGMP Snooping Vlan		
🖑 ERPS	* Vlan Mode	All Vlan 🔻	
I Mirror	 Vlan ID 	1	(1-4094)
Standard 1			

Figure 2 IGMP snooping global configuration

Parameter usage

ltem	Description
IGMP Snooping	Set the IGMP snooping global stats
Max Member Number	Set the IGMP snooping global max member number
TCN Querier Count	Set the IGMP snooping tcn querier count
TCN Querier Interval	Set the IGMP snooping tcn querier interval

If you want to configure parameters of IGMP snooping global, you can follow the following steps: (1) Select the IGMP snooping global stats in the "IGMP Snooping" dropdown box.

- (2) Enter the maximum number of IGMP members in the "Max member number" text box.
- Enter tcn querier count in the "TCN Querier Count" textbox. (3)
- (4) Enter tcn querier interval in the "TCN Querier Interval" textbox.
- (5)

Click the "Apply" button. Click the "Apply" button to confirm configure IGMP snooping global parameters. (6)

The operation is shown in figure 3, IGMP snooping globally configured the successful table entry is shown in figure 4.

VIP Snooping Global				
* IGMP Snooping	Enable		1	
* Max Member Number	2000		(1-2048, Default 2048) 2
* TCN Querier Count	5		(1-10, Default 2)	3
TCN Queries later al	100		(1-255 Default 10)	1,
 TCN Querier interval 	Apply 5		(1255, 2010) (10)	4
IGMP Snooping IGMP S	Apply 5			4
IGMP Snooping IGMP S IMP Snooping Global + IGMP Snooping	Apply 5 nooping Information Enable	tips	X	4
IGMP Snooping IGMP S IGMP Snooping Global • IGMP Snooping • Max Member Number	Apply 5 nooping Information Enable 2000	tips	× efault 204	B)
IGMP Snooping IGMP S IGMP Snooping Global IGMP Snooping IGMP Snooping Max Member Number TCN Querier Count	Apply 5 nooping Information Enable 2000 5	tips • Are you sure to configure?	× efault 204 uit 2)	8)

Figure 3 IGMP snooping global configuration operation

IGMP Snooping	IGMP Snooping Information
IGMP Snooping Globa	
IGMP Snooping	Enable
Max Member Number	200
TCN Querier Count	5
TCN Querier Interval	100

Figure 4 IGMP snooping global configuration information

14.1.2 IGMP Snooping VLAN Configuration

If you click "Multicast-> IGMP Snooping" in the title bar, the IGMP snooping VLAN configuration page appears, as shown in figure 5.

viP shooping vian		
 Vlan Mode 	All Vlan	*
* Vlan ID	1	(1-4094)
IGMP Snooping	Enable	¥
Discard Unkonwn	Disable	٣
Report Suppression	Disable	*
Fast Leave	Disable	*
Version	2	(1~3, Default 2)
Last Member Query Interval	1000	(1000-25500, Default 1000

Figure 5 IGMP snooping VLAN configuration

· Parameter usage

ltem	Description
Vlan Mode	Set the IGMP snooping VLAN mode(all VLAN or single VLAN)
Vlan ID	Set the IGMP snooping VLAN id on single VLAN mode
IGMP Snooping	Set the IGMP snooping VLAN stats
Discard Unknown	Set the IGMP snooping VLAN discard unknown stats
Report Suppression	Set the IGMP snooping VLAN report suppression stats
Fast Leave	Set the IGMP snooping VLAN fast leave stats
Version	Set the IGMP snooping VLAN version
Last Member Query Interval	Set the IGMP snooping VLAN last member query interval

If you want to configure parameters of IGMP snooping VLAN, you can follow the following steps:

- (1) Select the IGMP snooping VLAN mode in the "Vlan Mode" dropdown box.
- (2) Enter the IGMP snooping VLAN id in the "Vlan ID" textbox.
- (3) Select the IGMP snooping VLAN state in the "IGMP Snooping" dropdown box.
- (4) Select the IGMP snooping discard unknown stat in the "Discard Unknown" dropdown box.
- (5) Select the IGMP snooping report suppression stat in the "Report Suppression" dropdown box.
- (6) Select the IGMP snooping VLAN fast leave stat in the "Fast Leave" dropdown box.
- (7) Enter the IGMP snooping VLAN version in the "Version" textbox.
- (8) Enter the IGMP snooping VLAN last member query interval in the "Last Member Query Interval" textbox.
- (9) Click the "Apply" button.
- (10) Click the "Apply" button to confirm configure IGMP snooping VLAN parameters.

The operation is shown in figure 6, IGMP snooping VLAN configured the successful table entry is shown in figure 7.

IGMP Snooping Vlan							
* Vlan Mode	All Vlan			• 1			
* Vlan ID	1			(1-4094	2		
 IGMP Snooping 	Enable			• 3			
* Discard Unkonwn	Disable	6		- 4			
 Report Suppression 	Disable	8		· 5			
a Factlenia	Dirable			6			
- Fast Leave	Disable				_		
 Version 	1			(1~3, D	efault 2) 7		
* Last Member Query In	nterval 2000			(1000-2	5500, Default 1000)	8	
	Apply	9					
GMP Snooping Vlan							
* Vlan Mode	All Vlan			•			
* Vlan ID	10			(1-4094			
* IGMP Snooping	Enable	tips		×			
* Discard Unkonwn	Disable						
* Report Suppression	Disable		. Are you sure to co	nfigure?			
* Fast Leave	Disable		10				
1920 - M			Apply Ca	ncel			
* Version	1			(1~3, D	efault 2)		
* Last Member Query I	nterval 2000			(1000-2	5500, Default 1000)		
	Apply						
	F	igure 6 IGMP s	nooping VLAN co	onfiguration o	peration		
IGMP Spooping	IGMP Spooning Inform	ation					
sinophig		enell					
GMP Snooping Global							
IGMP Snooping	Enable						
Max Member Number	200						
ICN Querier Count	5						
ICN Querier Interval	100						
GMP Snooping Vlan						Last Marchae Que	
VLAN	Snooping Enable	Discard Unkown	Report Suppression	Fast Leave	Version	Last Wember Query	Opera
1	Enabled	Enabled	Enabled	Disabled	1	1000	Edit

Figure 7 IGMP snooping VLAN configuration information

Disabled

1

1000

Edit

Enabled

14.1.3 IGMP Snooping Information

Enabled

Enabled

2

If you click "Multicast-> IGMP Snooping Information" in the title bar, the IGMP snooping global information page, IGMP snooping groups information page and IGMP snooping VLAN information page appears, as shown in figure 8, figure 9 and figure 10.

Ethernet Status	IGMP Snooping	IGMP Snooping Inform	mation 2					
🕸 Link Aggregation								
III Storm Control	IGMP Shooping Global	Disable						
III Flow Control	Max Member Number	200						
Port Isolate	TCN Querier Count	5						
Port Detect	TCN Querier Interval	100						
∐ VLAN	IGMP Snooping Vlan							
B VLAN Classifier	V/ AN	Construction Freedom	Discol II down	B	5-10 L	Marchae	Last Member Query	0
🖵 MAC	VLAN	shooping Enable	Discard Unkown	Report Suppression	Past Leave	version	Interval	Operate
😫 Spanning Tree	1	Disabled	Enabled	Enabled	Disabled	1	1000	Edit
🐇 ERPS	2	Disabled	Enabled	Enabled	Disabled	1	1000	Edit
I Mirror	100	Disabled	Enabled	Enabled	Disabled	1	1000	Edit
备 Multicast 1	200	Disabled	Enabled	Enabled	Disabled	1	1000	Edit

Figure 8 IGMP snooping global information

• Parameter usage

ltem		Descr	iption					
IGMP Snooping		Display the IGMP snooping global stats						
Max Member Number		Display the IGMP snooping global max member number						
TCN Querier Count		Display the IGMP snooping tcn querier count						
TCN Querier Interval		Display the IGMP snoo	ping tcn querier interval					
IGMP Snooping Groups	Interface	Group Address	Expire Time					

No Data~

Figure 9 IGMP snooping groups information

• Parameter usage

lte	em		Description					
VL	AN		Display the VLAN ID for joining the IGMP snooping group					
Inte	rface	Di	Display the VLAN member port that have joined the IGMP snooping group					
Group	Address		Displays the IGMP snooping group address					
Expir	e Time		Display the expire time for the IGMP snooping group table entry					
IGMP Snooping Vla	n Snooping Enable	Discard Unkown	Report Suppression	Fast Leave	Version	Last Member Query Interval	Operation	
2	Enabled	Disabled	Disabled	Disabled	1	1000	Edit	

• Parameter usage

ltem	Description
Vlan Mode	Display the IGMP snooping VLAN mode
Vian ID	Display the IGMP snooping VLAN id on single VLAN mode
IGMP Snooping	Display the IGMP snooping VLAN stats
Discard Unknown	Display the IGMP snooping VLAN discasrd unknown stats
Report Suppression	Display the IGMP snooping VLAN report suppression stats
Fast Leave	Display the IGMP snooping VLAN fast leave stats
Version	Display the IGMP snooping VLAN version
Last Member Query Interval	Display the IGMP snooping VLAN last member query interval
Operation	Display that IGMP snooping VLAN table entries can be edited

If you want to modify the configuration to specify IGMP snooping VLAN, please click "Edit" button, the operation shown in figure 11, modify the specified IGMP snooping VLAN page appears, as shown in figure 12.

LAIN	Snooping Enable	Discard Unkown	Report Suppression	Fast Leave	Version	Last Member Query Interval	Operatio
	Enabled	Disabled	Enabled	Disabled	1	1000	Edit
	Enabled	Disabled	Disabled	Disabled	1	1000	Edit
		Figure 11	Modify IGMP sno	ooping VLAN o	operation		
MP Snoopinç	g Vlan						
* Vlan ID	2						
 IGMP Snoor 	ping	nable		٣			
Discard Unk	conwn	nable		*			
* Report Supj	pression	nable		*			
* Fast Leave	C	Disable		¥			
* Version	1			(1-	3, Default 2)		
	ar Quany Interval	000					

Figure 12 Modify IGMP snooping VLAN

• Parameter usage

ltem	Description
Vlan Mode	Display the IGMP snooping VLAN mode(all VLAN or single VLAN)
Vlan ID	Set the IGMP snooping VLAN id on single VLAN mode
IGMP Snooping	Set the IGMP snooping VLAN stats

FS

Discard Unknown	Set the IGMP snooping VLAN discasrd unknown stats
Report Suppression	Set the IGMP snooping VLAN report suppression stats
Fast Leave	Set the IGMP snooping VLAN fast leave stats
Version	Set the IGMP snooping VLAN version
Last Member Query Interval	Set the IGMP snooping VLAN last member query interval

If you want to modify parameters configuration of IGMP snooping VLAN, you can follow the following steps:

Select the IGMP snooping VLAN stat in the "IGMP Snooping" dropdown box. (1)

(2) Select the IGMP snooping discard unknown stat in the "Discard Unknown" dropdown box.

Select the IGMP snooping report suppression stat in the "Report Suppression" dropdown box. (3)

Select the IGMP snooping VLAN fast leave stat in the "Fast Leave" dropdown box. (4)

(5)

Enter the IGMP snooping VLAN version in the "Version" textbox. Enter the IGMP snooping VLAN last member query interval in the "Last Member Query Interval" textbox. (6)

(7) Click the "Apply" button to configure IGMP snooping VLAN parameters.

Click the "Apply" button to confirm configure IGMP snooping VLAN parameters. (8)

The operation is shown in figure 13.

IGMP Snooping Vlan		
* Vlan ID	2	
 IGMP Snooping 	Enable	• 1
* Discard Unkonwn	Enable	• 2
 Report Suppression 	Enable	* 3
* Fast Leave	Disable	• 4
* Version	2	(1-3, Default 2) 5
* Last Member Query Interval	3000	(1000-25500, Default 1000) 6
7	Apply Exit	
IGMP Snooping Vian		

Vlan ID	2		
IGMP Snooping	Enable		Y
Discard Unkonwn	Enable	tips	×
 Report Suppression 	Enable	Are you sure to configu	ire?
Fast Leave	Disable	8	
Version	2	Apply Cancel)
 Last Member Query Interval 	3000		(1000-25500, Default 1000)

Figure 13 Modify IGMP snooping VLAN

15. QOS

Quality of Service (QoS) can be used to give certain traffic priority over other traffic. Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped. With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

If you click "Configuration ->QOS" in the top control bar, the QOS configuration list page appears, as shown in figure 1.

Note: The S5800-48T4S model does not support QOS configuration through the Web Interface.

FS 55800-81F125			Monitor	Configuration	Maintenance	Network		
	-			1				
Ethernet Status	Global Configuration	n	Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit	
🕸 Link Aggregation								
🐹 Storm Control	Global Configuration	on	Dischler mit sie Mitchleren					
E Flow Control	QUS Enable	() Enable	Usable (Delault Disable)					
Port Isolate		Apply						
Port Detect								
H VLAN								
BB VLAN Classifier								
🖵 мас								
留 Spanning Tree								
48 ERPS								
I Mirror								
$\mathcal{Q}_{\mathfrak{a},\mathfrak{b}}$ Multicast								
a qos 2								
					1 0 0 0 1			

Figure 1 QOS list

15.1 Global Configuration

This section is used to enable or disable QOS global.

15.1.1 Current QOS Status

If you want to check QOS status on switch, you can click "QOS-> Global Configuration" in the title bar, the global configuration page appears, as shown in figure 2.



• Parameter usage

ltem	Description
Enable	Enable QOS globally
Disable	Disable QOS globally



If you want to change QOS status, please click to turn on or off, after that, click "Apply" to enable or disable QOS globally, the operation is shown in figure 3.

🐨 Ethernet Status	Global Configuration Interface Configuration Port Policer Traffic Shaping Congestion Manage Port rate limit
00 Link Aggregation	Global Configuration
3 Storm Control	* QOS Enable 1 O Enable (Default Disable)
I Flow Control	2 Arek
Port Isolate	
Port Detect	
La VLAN	
B8 VLAN Classifier	
MAC	
留 Spanning Tree	
4¢ ERPS	
Mirror	
Multicast	
R QOS	
I ALL	

Figure 3 Change QOS status operation

15.2 Interface Configuration

This section mainly describes how to view and configure QOS property on interface.

15.2.1 Interface Configuration View

If you click "QOS -> Interface Configuration" in the title bar, the QOS interface configuration page appears, as shown in figure 4.

FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network		Save admin Logout
	E.						
Ethernet Status	Global Configuration 2	Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit	
🕸 Link Aggregation	L						
3 Storm Control	QoS Interface Configuration						
1 Flow Control	Edit						
Port Isolate	Interface Name	Trust Status					Operation
Port Detect	eth-0-1	COS					Edit
L VLAN	🗋 eth-0-2	COS					Edit
B VLAN Classifier	🗋 eth-0-3	COS					Edit
MAC	🗌 eth-0-4	COS					Edit
留 Spanning Tree	🗌 eth-0-5	cos					Edit
√a ERPS	🗌 eth-0-6	COS					Edit
Mirror	eth-0-7	COS					Edit
S Multicast	🗆 eth-0-8	COS					Edit
a qos 1	🗌 eth-0-9	COS					Edit
🖄 ACL	🗋 eth-0-10	COS					Edit

Figure 4 QOS interface configuration

• Parameter usage

ltem	Description
Interface Name	Display the number of interface
Replace COS	Display enable or disable replace the cos field in packets on egress
Replace DSCP	Display enable or disable replace the dscp field in packets on egress
Trust Status	Display the trust type on port
Operation	Display that interface entries can be edited

15.2.2 Interface Attribute Configuration

If you want to enter the interface attribute configuration page, you can follow the following steps:

- Select this specified Interface which you want to configure. (1)
- Click "Edit" button. (2)

The operation is shown in figure 5. and then the interface QOS configuration page appears, as shown in figure 6.

FS 55800-8TF125		Monitor	Ç Configuration	X Maintenance	Network		Save admin Logout
Ethernet Status	Global Configuration	Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit	
00 Link Aggregation							
31 Storm Control	QoS Interface Configurat	ion					
Flow Control	Edit						
Port Isolate	Interface Name	Trust Status					Operation
Port Detect	1 eth-0-1	COS					Edit
LL VLAN	eth-0-2	COS					Edit
B VLAN Classifier	🗌 eth-0-3	COS					Edit
🖳 MAC	🗌 eth-0-4	COS					Edit
😫 Spanning Tree	eth-0-5	COS					Edit
40 ERPS	🗌 eth-0-6	cos					Edit
I Mirror	🗌 eth-0-7	cos					Edit
and Multicast	eth-0-8	COS					Edit
a qos	🗌 eth-0-9	cos					Edit
🖄 ACL	🗌 eth-0-10	cos					Edit

Figure 5 Interface QOS configuration operation

FS 55800-8TF125			Monitor	Configuration	Maintenance	Network			
Ethernet Status	Global Configuration	n Interfac	e Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit		
🕸 Link Aggregation									
X Storm Control	Interface Security	Configuration -							
E Flow Control	Interface Name	eth-0-1							
Port Isolate									
Port Detect	Trust Status	COS			Ŧ				
		Apply	Back						
B0 VLAN Classifier									
MAC									
😫 Spanning Tree									
🎸 ERPS									
Mirror									
💑 Multicast									
🔒 qos									

Figure 6 Interface QOS configuration

· Parameter usage

Item	Description
Interface Name	Display the number of interface
Trust	Set trust type on port

If you want to modify the trust status, you can follow the following steps:

Select the Trust type in the "Trust Status" dropdown box.
 Click the "Apply" button to apply all the property.

The operation is shown in figure 7, trust status configuration success table entry is shown in figure 8.

Global Configuration	1	Interface Configuration	Port Policer	Traffic Shaping	Congestion Manage	Port rate limit	
Interface Security (Configur	ation					
Interface Name:	eth-0-1						
* Trust Status: 1	IP-PREC	2		~			
2	Apply	Back					

Figure 7 Modify the trust status configuration

Global Configuration	Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit	
QoS Interface Configurat	tion					
Interface Name	Trust Status					Operation
🗋 eth-0-1	IP-PREC					Edit
eth-0-2	COS					Edit
□ eth-0-3	COS					Edit
🗌 eth-0-4	COS					Edit
🗋 eth-0-5	COS					Edit
🗋 eth-0-6	COS					Edit
🗌 eth-0-7	COS					Edit
🗋 eth-0-8	COS					Edit
🗋 eth-0-9	COS					Edit
🗌 eth-0-10	COS					Edit

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Figure 8 Trust status configuration information

15.3 Port Policer

This section mainly describes how to view and configure port policer for an interface matching all traffic transmitted and received in different direction.

15.3.1 Port Policer View

If you click "QOS -> Port Policer" in the title bar, the QOS port policer configuration page appears, as shown in figure 9.

Global Cont	iguration	Interface Configuration Port Policer	Traffic Shaping Cong	estion Manage	ment Port Rate Limit		
Port Policer Mode	• View Port Pol	icer O Configure Port Policer (Optional mu	ltiple port)				
Panel		675 55800-87F125			10/10/1000 EASE-T	1+2,2,4 3-24,7 8 	94*(51 12, 134*(55 16, 174*(55 20) 100/100 for the set of the set
Settings	Direction	🛛 İnput		Direction	Output		
	Color Mode	🔾 Color Aware 🛛 🛞 Color Blind		Color Mode	⊖ Color Aware 🛞 Color Blind		
	CIR			CIR			
	CBS		(0~8000000)	CBS		(0~8000000)	
	Туре	O EBS		Туре	O EBS		
	EBS		(0~8000000)	EBS		(0-8000000)	
	Туре	[☉] PIR		Type	O PIR		
	PIR			PIR			
	PBS		(0~8000000)	PBS		(0~8000000)	
	Туре	_O EIR		Туре	O EIR		
	EIR			EIR			
	EBS			EBS			
	Drop Color	Red Vellow		Drop Color	Red Vellow		
	Use L3 Length	Ves ® No					

Figure 9 QOS port policer configuration

Parameter usage

ltem	Description					
Direction	Choose the direction to limit the traffic entering the interface					
Color Mode	Choose color aware or color blind mode policer					
CIR	Commit Information Rate with the range of 0 to 10,000,000 kbps					
CBS	Commit Burst Size with the range of 0 to 8,000,000 bytes					
Туре	Choose EBS					
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes					
Туре	Choose PIR					
PIR	Peak Information Rate with the range of 0 to 10,000,000 kbps					
PBS	Peak Burst Size with the range of 0 to 8,000,000 bytes					
Туре	Choose EIR					
EIR	Excess Information Rate with the rang of 0 to 10,000,000 kbps					
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes					
Drop Color	Drop color configuration includes yellow and red					
Use L3 Length	Use layer 3 length for policing					

15.3.2 Modify Port Policer

If you want to modify the port policer configuration, please click "Configure Congestion" button, the operation is shown in figure 10. and then the port policer configure page appears, as shown in figure 11.

FS [55800-8TF125]					Monitor	Configuration	X Maintenance	Networ	4			Save admin Logout
Thernet Status	Global Configu	ration Inte	rface Configuration	Port Policer	Traffic Shaping	Congestion M	anagement	Port Rate Limit				
00 Link Aggregation	Port Policer											
)其 Storm Control	Mode	○ View Port Pol	icer 1 Configure Po	rt Policer (Ontional m	tion slott							
E Flow Control		0.111.111.1		a contra copination (
Port Isolate	Panel	CYL 2AV	NOR NOR NOR NOR PWARTPWARTPLACE AND									
Dert Detect						14.72 347 F	+ 14+6 74+1 + + +	14 W2 34 W4	54.76 7A.78		14.9	
님 VLAN			- GFS			WITTH STT		250282	25/2/8/2		7.57	
BR VLAN Classifier			US8 58600-877125			10/100	/1000 BASE-T		Markey Contraction			100/1000 BASE-X
🖓 мас												
😭 Spanning Tree	Settings	Direction	🗌 İnput					Direction	Output			
d_{0}^{a} ERPS		Color Mode	O Color Aware	Color Blind				Color Mode	O Color Aware	Color Blind		
Mirror		* CIR				(0-10000000)		* CIR				
$_{0}\mathbb{P}_{0}^{\mathbb{P}}$ Multicast		CBS						CBS				
A QOS		Type	○ FRS					Type	O FRS			
C ACL			G					. See	0.01			
		EBS						685				
		Туре	O PIR					Type	O PIR			
		PIR						PIR				
		PBS				(0-8000000)		PBS				(0-8000000)
		Туре	⊖ EIR					Туре	⊖ EIR			
		EIR						EIR				
						Copyright	© 2009-2020 F5.COM	Inc . All Rights Rei	served,			

Figure 10 Port policer configure operation

FS SSB00-BTF125			Monitar	Configuration	% Maintenance	netwood	λ.	Save admin Logout
🐨 Ethernet Status	Global Configuration Interface Con	figuration Port Policer	Traffic Shaping	Congestion Ma	nagement	Port Rate Limit		
(I) Link Aggregation	Port Policer							
X Storm Control	Mode OView Port Policer	Configure Port Policer (Optional m	ultiple port)					
Flow Control								
Port Detect	555 144 PMIL PMIL 257	C6 402		14.97 14.94	14 TE 74 TE	14.92 34.94	SATE 7ATE	
A VLAN		() FS		Total Total	Store Stores	250282		151250 022250 022250
88 VLAN Classifier	EXH USO	\$8800-877125		10/100/	1000 BASE-1	1111 2111 100/1000 B	MAR X	100/1000 BASE-X
S MAC								
12 Spanning Tree	Settings Direction	ut				Direction	Output	
48 ERPS	Color Mode O Colo	or Aware Color Blind				Color Mode	O Color Aware Color Blind	
Mirror	* CIR					* CIR		
$\beta_{\rm B}$ Multicast	CBS			(0-8000000)		CBS		(0-8000000)
& QOS	Type O EBS					Туре	O EBS	
2 ACL	EBS			(0-8000000)		EBS		(0-8000000)
	Type O PIR					Туре	O PIR	
	PIR			(0-10000000)		PIR		
	PBS			(0-8000000)		PBS		(0-8000000)
	Type O EIR					Туре	⊖ EIR	
	EIR					EIR		

Figure 11 Port policer configure

• Parameter usage

ltem	Description					
Direction	Choose the direction to limit the traffic entering the interface					
Color Mode	Choose color aware or color blind mode policer					
CIR	Commit Information Rate with the range of 0 to 10,000,000 kbps					
CBS	Commit Burst Size with the range of 0 to 8,000,000 bytes					
Туре	Choose EBS					
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes					
Туре	Choose PIR					
PIR	Peak Information Rate with the range of 0 to 10,000,000 kbps					

FS

Item	Description					
PBS	Peak Burst Size with the range of 0 to 8,000,000 bytes					
Туре	Choose EIR					
EIR	Excess Information Rate with the rang of 0 to 10,000,000 kbps					
EBS	Excess Burst Size with the range of 0 to 8,000,000 bytes					
Drop Color	Drop color configuration includes yellow and red					
Use L3 Length	Use layer 3 length for policing					

- If you want to modify the port policer, you can follow the following steps:(1) Choose one port to display the configuration information.
- (2) Choose the direction to limit the traffic entering the interface.
- Choose color aware or color blind mode policer. (3)
- Commit Information Rate with the range of 1 to 10,000,000 kbps. (4)
- Commit Burst Size with the range of 0 to 16,000 bytes. Choose type of EBS or PIR or EIR. (5)
- (6)
- Configure parameters of QoS on port. Choose drop color configuration includes yellow and red. (7)
- (8)
- (9) Choose whether use layer 3 length for policing.
- (10) Click the "Apply" button to apply all the property.

The operation is shown in figure 12, port policer configuration success table entry is shown in figure 13.

	Port Policer						
🕑 Ethernet Status	Mode	O View Port Pol	icer Configure Port Policer (Optional multiple				
(I) Link Aggregation	Panel						
3 Storm Control	1			14.72 14.74 14	14 74 74 14 72 1	A 74 5476 7678	
Flow Control		CON TITLE	(G) FS	Rectang Street St.		\$0 2322-20	232280 23280 23250
Port Isolate		ETH W	58000-8TF125	10/100/100	BASE-T	100 1000 BASE-X	1007 1000 BASE A
Port Detect							
La VLAN	Settings 2	Direction	⊡Input		Direction	C Output	
88 VLAN Classifier	3	Color Mode	🔾 Color Aware 🛛 🛞 Color Blind		Color Mode	🔿 Color Aware 🛛 🛞 Color Blind	
MAC		- CIR			+ CIR		(0-10000000)
12 Spanning Tree		CBS			CBS		0-1000000
44 ERPS					22		
🗇 Mirror	4~7	Type	Oraz		Type	Otas	
A Multicast		EBS			EBS		(0~8000000)
A QOS	ę	Туре	⊖ PIR		Type	○ PIR	
2 ACL		PIR		(0-10000000)	PIR		(0-1000000)
		PBS		(0-8000000)	PBS		(0-8000000)
		Туре	OEIR		Туре	OER	
		EIR		(0-10000000)	EIR		(0-10000000)
		EBS		(0-8000000)	EBS		(0-8000000)
	8	Drop Color	🙍 Red 🛛 Yellow		Drop Color	🗑 Red 🛛 Yellow	
	9	Use L3 Length	🔾 Yes 🕘 No				
		10	Apply Delete	Copyright © 2009	-2020 FS.COM Inc. All Ris	jhts Reserved.	

Figure 12 Modify the port policer configuration

FS SS800-BTF125			E Mor	itor Configuration	Maintenance Retwork		
		етн 1000	G/FS				
🕙 Ethernet Status		-	Ute	10/100/1	1000 BASE-T 100/1000 BASE-X		100/1000 BASE-X
(I) Link Aggregation	Sattings	Direction	Cleart		Direction	Outrat	
翼 Storm Control	soungs	Color Mode	Color Aware		Color Mode	Color Aware Color Blind	
Flow Control		Color mode			COURT MODE		
Port Isolate		- CIR			- CIR		(0-10000000)
D Port Detect		CBS		(0-800	10000) CBS		(0-8000000)
≟i VLAN		Туре	⊖ EBS		Туре	⊖ EBS	
88 VLAN Classifier		EBS			0000) EBS		(0~8000000)
MAC MAC			ORR		Tuna	() PIP	
웹 Spanning Tree		type	UHK		type	() PIK	
4¢ ERPS		PIR			100000) PIR		(5-10000000)
@ Mirror		PBS		(0-800	20100) PBS		(00000001-07)
\mathcal{J}_h Multicast		Туре	OER		Type	⊖ EIR	
A QOS		EIR			1000000) EIR		(0-10000000)
[/] ACL		1000					
		EBS			10000) EBS		(0-000000)
		Drop Color	Red O Yellow		Drop Color	Red () Yellow	
		Use L3 Length	🔾 Yes 💿 No				

Figure 13 Port policer configuration information

15.4 Traffic Shaping

This section mainly describes how to view and configure shaping for a queue of a port in absolute value mode.

15.4.1 Traffic Shaping View

If you click "QOS ->Traffic Shaping" in the title bar, the QOS traffic shaping configuration page appears, as shown in figure 14.

FS 55800-8TF125	💭 😋 💥 📅 Montor Configuration Martenanca Hestook	Save admin Logout
	and the standard standard standard standard	
Ethernet Status	Global Configuration Interface Configuration Port Policer Traffic Shaping Congestion Management Port Rate Limit	
🙌 Link Aggregation	Traffic Shanlog	
3% Storm Control	Mode View Traffic Stanling Ocentraum Traffic Stanling (Chefraum Traffic Stanling)	
Flow Control		
🕀 Port Isolate	Panel St. His Yest Hell StCK HO	
Port Detect		1111 1111 1111 1111
닖, VLAN	GFS THE THE THE THE THE THE THE THE THE THE	TATATATA DA TATATA
88 VLAN Classifier		- 100/1000 BASE-X -
🖵 MAC		
😫 Spanning Tree	Settings Queue QR (0-1000000, Unit: Ma(V)) PR (0-1000000, Unit: Ma(V) and be smaller than CR)	
4¢ ERPS	Queue 0	
I Mirror	Quirue 1	
an Multicast		
@ QOS	Qurie Z	
Z ACL	Qurue 3	
	Qurve 4	
	Queve 3	
	Quoue 6	
	Queen 7	
	Copyright © 2009-2020 FS.COM Inc. All Rights Reserved.	

Figure 14 QOS traffic shaping configuration

Parameter usage

ltem	Description					
Queues	The id of queue for port. The range of queue id is from 0 to 7					
CIR	The value for commit information rate with the range of 0 to 10,000,000					
PIR	The value for peak information rate with the range of 0 to 10,000,000. If this value is omitted, it will be same as cir					

15.4.2 Modify Traffic Shaping

If you want to modify the Traffic Shaping configuration, please click "Configure Congestion" button, the operation is shown in figure 15.

And then the traffic shaping configure page appears, as shown in figure 16.

FS 55800-87F125	Noritor Configuration Maintenance Neuroph	Save admin Logout
🗑 Ethernet Status	Global Configuration Interface Configuration Post Policer Traffic Staging Congestion Management Post Rate Limit	
(Ink Aggregation	Talla Daulae	
3% Storm Control	Mode O'View Traffic Shaping Configure Traffic Shaping (Optional multiple port)	
Flow Control Port Isolate	Farel 15. 10. 701 702 CO. 40	
Port Detect		
UAN VIAN		
₩ MAC		
留 Spanning Tree	Settings Queue CR (1-1000000, Unit kisi/u) PR (1-1000000, Unit kisi/u, cannot be unaffer Han (18)	
≪ ERPS	Dana 1	
$\frac{\partial}{\partial a}$ Multicast	0.0002	
A QOS	Quee 3	
	Quite 4	
	Quine 5	
	Quite 6	
	Qurve 7	

Figure 15 Traffic shaping configure operation

FS 55800-8TF125	Monitar Configuration Maintenance Network	igout
😳 Ethernet Status	Global Configuration Interface Configuration Port Policer Traffic Shaping Congestion Management Port Rate Limit	
(i) Link Aggregation	Totlle Chusica	
3% Storm Control	International Statement	
Flow Control	INTE Creat Letter and and Constant and Constant Constan	
Port Isolate	Panel B B B B B B B B B B B B B B B B B B B	
Port Detect		
HA VLAN		
St VLAN Classifier		
💭 MAC		
留 Spanning Tree	Settings Queue OR (0-1000000, Unit: Mal/s) PR (0-1000000, Unit: Mal/s) PR (0-1000000, Unit: Mal/s, cannot be smaller than CI2	
🐇 ERPS	Queue 0	
Mirror	Ourse 1	
🖧 Multicast		
A QOS	Same 2	
2 ACL	Queue 3	
	Queue 4	
	Queue 5	
	Queue 6	
	Querue 7	

Figure 16 Traffic shaping configure

Parameter usage

ltem	Description				
Queues	The id of queue for port. The range of queue id is from 0 to 7				
CIR	The value for commit information rate with the range of 0 to 10,000,000				
PIR	The value for peak information rate with the range of 0 to 10,000,000. If this value is omitted, it will be same as cir				

If you want to modify the traffic shaping, you can follow the following steps:(1) Choose one port to display the configuration information.

(2)

Modify Queue Settings. Click the "Apply" button to apply all the property. (3)

The operation is shown in figure 17, traffic shaping configuration success table entry is shown in figure 18.

FS 55800-877125		Configuration	X Haintenance Network	Save admin Logout
Ethernet Status Link Apprendices	Global Config	ation Interface Configuration Port Policer Traffic Shaping Congestion Manag	gement Port Rate Limit	
Storm Control	Traffic Shaping Mode	O View Traffic Shaping Configure Traffic Shaping (Optional multiple port)		
Port Isolate Port Detect VLAN VLAN Classifier	Panel 1			
MAC Spanning Tree CRPS	Settings	Queue QR (0-10000000, Unit: Maly) PR (0-10000000, Unit: Maly) Queue 0	c sampat be smaller than CID	
Mirror Multicast QOS ACL	2	Conver2 Conver2 Conver3 Conver		
		Queue 6		
		Queen 7		
		3 Apply	rt © 2008-2020 FS.COM Inc. All Rights Reserved.	

Figure 17 Modify the traffic shaping configuration

FS [\$5800-8TF125]			Monitor Configuration	Haintenance Network	Save admin togout
Ethernet Status	Global Confi	guration Interface Configuration Po	rt Policer Traffic Shaping Congestion Manag	ement Port Rate Limit	
99 Link Aggregation					
II Storm Control	Traffic Shaping	9 View Teallie Chaples Configure Teallie S	A sector of the state of the sector		
Flaw Control	mode	O view manie anapirity	advard Coloronal merutine traini		
Port Isolate	Panel	THE AND AN AN AN AN AN THE FARMMAN PRODUCTION AND			
Port Detect		CON THE			
🗄 VLAN		ETH CFS	100		
E VLAN Classifier		HE USE		10/100/1000 EASE-T 100/1000 EASE-X	100/1000 BASE W
© MAC	Settings	Queue CIR IS-10000000 Unit-Hidday	PIE IN LITERATION LITER HOUSE		
🗄 Spanning Tree			200000		
4 ERPS		Queue 0 100000	20000		
D Mirror		Queue 1			
\mathbb{P}_{n} Multicast		Queue 2			
# QOS		Queue 3			
🖾 ACL					
		Queue 4			
		Queue 5			
		Queue 6			
		Queue 7			
		Port Shape			
		Apply			
			Copyright	© 2009-2020 FS.COM Inc . All Rights Reserved.	

Figure 18 Traffic shaping configuration information

15.5 Congestion Manage

This section mainly describes how to view and configure the WDRR scheduling weight and class for each queue.

15.5.1 Congestion Manage View

If you click "QOS -> Congestion Manage" in the title bar, the QOS congestion manage configuration page appears, as shown in figure 19.

FS [\$5800-8TF125]				Monitor	Configuration	* Maintenance	Network	Save admin Logout
Ethernet Status	Global Conf	iguration Interface Configuration	Port Policer T	raffic Shaping	Congestion Management	Port Rate I	Limit	
00 Link Appregation								
X Storm Control	Congestion N	fanagement						
E How Control	Mode	View Congestion Management O	Configure Congestion Mana	igement (Optional				
Port Isolate	Panel	SVS FAARWEISVARUSSEE NO					and the second second second second second second second second second second second second second second second	
Port Detect		and all the			1472 3474	POTO I	10.72 JATA 34.76 74.78	
U VLAN		GFS			BALL BALL	NAME AND A	19113C 19173C	777752 257757 25757
VLAN Classifier		S5800-8TF125			10/100/1	DOD BASE-T	100-7030 BASE-X	Lineared Research (Research Research Re
MAC MAC	8 1							
Spanning Tree	settings	If several queues are mapped to same + Class		• Queues	DRR Weight (1~100)			
E ERPS				Ourse 0				
I Mirror				QUIVES V				
R Multicast				Queues 1	1			
a qos			*	Queues 2	1			
21 ACL				Queues 3	1			
		4	×	Queues 4	1			
		5		Queues 5	1			
		8	*	Queues 6	1			
			*	Queues 7	1			
					Copyright © 2009	-2020 FS-COM Inc	: . All Rights Reserved.	

Figure 19 QOS congestion manage configuration

• Parameter usage

ltem	Description
Queues	The id of queue for port. The range of queue id is from 0 to 7
Class	The class level of queue with the range of 0 to 7
DRR Weight	The value of DRR weight with the range of 1 to 100

15.5.2 Modify Congestion Manage

If you want to modify the congestion manage configuration, please click "Configure Congestion" button, the operation is shown in figure 20. and then the congestion manage configure congestion page appears, as shown in figure 21.

FS [\$5800-81F125]				Monitar	Configuration	* Maintenance	network.	Save admin Logout
TT Different Citation	Global Confi	uration Interface Configuration	Port Policer	Traffic Shanion	Constant Management	Root Rate Limit		
(*) Link Aggregation	onooar conny	pranter conspiration	PULPUIG	manic anapang	congestion management	Port Hate Com		
31 Storm Control	Congestion M	anagement	- Connection Man	10-2	and the second se			
Flow Control	mode	O view congestion management -	ningure congestion was	agement (operation	manifest Provid			
🗎 Port Isolate	Panel	SIN FAMPHERSPREZEDX IND			14.72 34.74		2 1474 3478 7478	JATIOLATIC DATMENTS DATMENTS
Port Detect								030030 030130 030030
U VLAN		ETH			10/100/1	IDIO BASE-T	10 1011 1010 HASE-X	100/1000 BASE #
☑ MAC								
Spanning Tree	Settings	If several queues are mapped to same cla • Class		WDRIL Otherwise the Queues	ey are scheduled as SP with cle DRR Weight (1~100)			
4: ERPS		0	-	Queues 0	1			
⊕ Mirror		1	*	Queues 1	1			
A Multicast		2	*	Oursear 2	1			
e dos		-		Queuesz				
		3		Queues 3	1			
		4	*	Queues 4	1			
		5	*	Queues 5	1			
		6	*	Queues 6	1			
		7		Queues 7	1			
		Apply						
					Copyright © 2009	-2020 FS.COM Inc . All	Rights Reserved.	

Figure 20 Congestion manage configure operation



Figure 21 Congestion manage configure

Parameter usage

Item	Description
Queues	The id of queue for port. The range of queue id is from 0 to 7
Class	The class level of queue with the range of 0 to 7
DRR Weight	The value of DRR weight with the range of 1 to 100

If you want to modify the congestion manage, you can follow the following steps:

- (1) Choose one port to display the configuration information.
- Modify Class Settings. (2)
- (3)
- Modify DRR Weight Settings. Click the "Apply" button to apply all the property. (4)
- The operation is shown in figure 22, congestion manage configuration success table entry is shown in figure 23.

FS SS800-8TF125				Monitor	Configuration	* Maintenance	Network	Save admin Logout
Ethernet Status Link Aggregation	Global Config	uration Interface Configuration Port Policer	Traffic	Shaping	Congestion Management	Port Rate	Limit	
第 Storm Control 回 Flow Control	Congestion Ma Mode	nagement O View Congestion Management Configure Congestion	Manageme	nt (Optional n	nultiple part)			
Port Isolate Port Detect VLAN VLAN VLAN Classifier	Panel 1							
MAC Spanning Tree	Settings	If several quesies are mapped to same class, they are schedul - Class	ed as WDRI	C Otherwise th	vey are scheduled as SP with clar DRR Weight (1–100)			
4 ERPS 部 Mirror		0		Queues 0	a 3			
A Multicast	2	[1] [2] *]		Queues 2	1			
2 ACL	-	3	3	Queues 3 Queues 4	1			
		5 *		Queues 5	1			
		6. • 7. •		Queues 6 Queues 7	1			
	4	Apply						
					Copyright © 2009-	2020 FS.COM Is	ic. All Rights Reserved.	

Figure 22 Modify the congestion manage configuration



FS 55800-8TF125				Monitor	Configuration Maintenance	П Network	Save admin Logout
③ Ethernet Status	Global Confi	guration Interface Configuration	Port Policer Tr	affic Shaping	Congestion Management Port Rate U	imit	
00 Link Aggregation							
31 Storm Control	Congestion M	lanagement					
Flow Control	Mode	O View Congestion Management Co	nfigure Congestion Manag	gement (Optional)			
Port Isolate	Panel	SIS LAAPWINWESSCORD					
Port Detect		con 👘			Part in the tart		· · · · · · · · · · · · · · · · · · ·
A VLAN		ETH GFS			NAME AND ADDRESS OF	100 100 100 100 100	
11 VLAN Classifier		USS USS			10/100/1000 BASE-T	100/1000 BASE-X	100/1000 BASE-H
	Settinos						
11 Spanning Tree	second s	- Class		• Queues	DRR Weight (1~100)		
42 ERPS		0	*	Oueues 0	1		
Mirror				201000	1		
A Multicast		1	*	Queues 1	80		
a qos		2	*	Queues 2	1		
ET ACL		3	-	Queues 3	1		
		4	*	Queues 4	1		
		5	-	Queues 5	1		

Figure 23 Congestion manage configuration information

15.6 Port Rate Limit

This section mainly describes how to view and configure port rate limit.

15.6.1 Port Rate Limit View

If you click "QOS ->Port rate limit" in the title bar, the port rate limit configuration page appears, as shown in figure 24.

				Manitor	Configuration	* Maintenanze	Network	
_								
met Status	Global Configuration	Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit		
Aggregation	Dea Data Maria							
n Control	Port Rate Umit							
Control	(Refresh)							
olate	Interface Name	Input		Output				Operatio
etect	eth-0-1							Edit
	□ eth-0-2							Edit
lassifier	eth-0-3							Edit
	eth-0-4							Edit
ing Tree	eth-0-5							Edit
	□ eth-0-6	н.						Edit
	eth-0-7	÷		-				Edit
ast	eth-0-8							Edit
	eth-0-9	-		÷				Edit
	🗇 eth-0-10	-		-				Edit
	🗆 eth-0-11							Edit
	□ eth-0-12			-				Edit
	eth-0-13			-				Edit
	eth-0-14							Edit
	eth-0-15	4		-				Edit
	eth-0-16	2		-				Edit
	□ eth-0-17							Edit
	C - + 0.10							

Figure 24 Port rate limit configuration

Parameter usage

Item	Description
Interface Name	Display the number of interface
Input	Input speed limit, range 8-10 million, unit kbps
Output	Output speed limit, range 8-10 million, unit kbps
Operation	Display that static routing table entries can be edited

15.6.2 Modify Port Rate Limit

Follow the following steps, you can enter the port rate limit configuration page:

(1) Select this specified Interface which you want to configure.

(2) Click "Edit" button.

The operation is shown in figure 25. and then the port rate limit configure page appears, as shown in figure 26.

Global Configuration	Interface Configuration	Port Policer	Traffic Shaping	Congestion Manage	Port rate limit	
Port rate limit	sh					
Interface Name	Input	Output				Operation
1 @eth-0-1						Edit
□eth-0-2						Edit
□eth-0-3		55				Edit
□eth-0-4						Edit
□eth-0-5	(55)	-				Edit
□eth-0-6						Edit
□eth-0-7						Edit
□eth-0-8		55				Edit
□eth-0-9						Edit
eth-0-10						Edit

Figure 25 Port rate limit configure operation

Global Configura	tion Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit	
Port Rate Limit Co	nfiguration					
Interface Name	eth-0-1					
Innut	Disabled O Peterlimit					
Rate limit						
Output	⊚ Disabled _○ Rate limit					
Rate limit	0					
	Apply Back					

Figure 26 Port rate limit configuration

· Parameter usage

ltem	Description
Interface Name	Display the number of interface
Input	Input speed limit, range 8-10 million, unit kbps
Output	Output speed limit, range 8-10 million, unit kbps

If you want to modify the port rate limit, you can follow the following steps: (1) Choose Disbale or Rate limit in the "Input" radio button.

- Enter rate in the "Rate limit" textbox. (2)
- Choose Disbale or Rate limit in the "Output" radio button. (3)
- (4)
- Enter rate in the "Rate limit" textbox. Click the "Apply" button to apply all the property. (5)

The operation is shown in figure 27, port rate limit configuration success table entry is shown in figure 28.

Global Configuration	Interface Configuration	Port Policer	Traffic Shaping	Congestion Management	Port Rate Limit	
Port Rate Limit Configurati	ion					
Interface Name eth-0-	1					
Input O Disab	led 💿 Rate limit 🛛 1					
Rate limit 1000			(0-1000000) 2			
Output 🛛 Disab	led Rate limit					
Rate limit 1000			(0-10000000) 4			
5 Appl	y Back					

Figure 27 Modify the port rate limit configuration

Global Configuration	Interface Configuration Po	rt Policer Traffic Shaping	Congestion Management	Port Rate Limit
Port Rate Limit				
Edit (Refresh)				
Interface Name	Input	Output		Operation
eth-0-1	1000 kbps	1000 kbps		Edit
eth-0-2				Edit
🗆 eth-0-3		144		Edit
🗆 eth-0-4				Edit
eth-0-5				Edit
eth-0-6	(C)			Edit
🗆 eth-0-7				Edit
🗆 eth-0-8				Edit
eth-0-9				Edit
eth-0-10	~			Edit
🗆 eth-0-11				Edit
🗆 eth-0-12		1.00		Edit
🗆 eth-0-13	-			Edit
□ eth-0-14		1.00		Edit
🗆 eth-0-15				Edit
🗆 eth-0-16		1.77		Edit
🗆 eth-0-17				Edit
eth-0-18		1.77		Edit

Figure 28 Port rate limit configuration information

16. ACL

If you click "Configuration -> ACL" in the top control bar, the ACL configuration list page appears, as shown in figure 1.

FS 55800-8TF12S		Monitor	Configuration	X Maintenance	Network		
			1				
Ethernet Status	Access Control List Clas	s Map Policy Map					
帥 Link Aggregation							
X Storm Control	ACL						
Flow Control	Create						
Port Isolate	Name Name		Туре			Operation	
Port Detect							
님 VLAN							
B VLAN Classifier				100			
🖵 мас				No data-			
🖺 Spanning Tree							
🆧 ERPS							
Mirror							
en Multicast							
a qos	ACL Rules						
ACL 2	Current ACL Name: T	pe: (click the [Editorial Rules]					
			Copyright (C) 2009-2020 FS.COM Inc .	All Rights Reserved.		
		_					

Figure 1 ACL information

16.1 Access Control List

If you click "ACL -> Access Control List" in the top control bar, the access control list configuration list page appears, as shown in figure 2.

Ethernet Status	Access Control List 2	Ilass Map Policy Map	
00 Link Aggregation			
3 Storm Control	ACL		
Flow Control	Create		
Port Isolate	Name	Туре	Operation
Port Detect			
🗄 VLAN			
Bo VLAN Classifier		100	
MAC		No data~	
🖽 Spanning Tree			
4¢ ERPS			
Mirror			
🖧 Multicast			
a QOS	ACL Rules		
🖾 ACL 1	Current ACL Name:	Type: (click the [Editorial Rules] button in the ACL operation bar to configure this.)	
	Add (Delete)	Copyright © 2009-2020 FS.COM Inc. All Rights Res	served.

Figure 2 Access control list information

16.1.1 ACL Configuration

ACL provide two basic configuration functions, creating and removing ACL.

If you want to create an ACL, here are the steps:

If you click the "Create" button, you can create ACL. The operation is shown in Figure 3, and then the ACL configuration page appears, as shown in Figure 4.

ACL		
Create		
Name	Туре	Operation
ac1	mac	Editorial Rules
a1	ip	Editorial Rules

Figure 3 ACL creation process

Create Access List		
* ACL Name	Please enter	
* Туре	ip	*
	Create	

Figure 4 ACL create page

· Parameter usage

Item	Description
ACL Name	Enter the acl name
Туре	Select the acl type

If you want to configure ACL, perform the following steps:

- (1)
- In the "ACL name" text box, enter ACL name. Select the type in the "type " drop-down box. (2)
- (3) Click "Create " button.
- Confirm the submission configuration and click the "Create " button. (4)

The operation is shown in figure 5, and the ACL configuration success entry is shown in figure 6.

Create Access List			
- ACL Name 1 a1			
• Type 2 ip	*		
2 Create Exit			
	tips	×	
	Are you sure to con	igure?	
	Figure 5 Create ACL o	onfiguration	
ACI			
Create Delete			
Name	Туре	Operation	

Figure 6 New ACL information

Editorial Rules

Editorial Rules

If you want to delete the ACL, here are the steps:

- Click the checkbox to select ACL which are need to be deleted as the figure below. (1)
- Click "Delete" button. (2)

ac1

🔲 a1

After clicking "Delete", the page as shown in figure 7 appears, and if you click the "Confirm" button, you can delete it. (3)

mad

ip

Access Control List Class Map Policy Map			
ACL Delete			
2	tips	×	Operation Editorial Rules
1 🖉 acl2	Are you sure to delete selected ACL?		Editorial Rules
ACL Rules Current ACL Name: ac1 Type: mac(click the (Editorial Rules) but	Confirm		
Add Delete	ACL Entry		

Figure 7 Delete ACL

16.1.2 ACL Rules

ACL rules provides two basic configuration functions: creating and deleting ACL rules.

If you want to create an ACL rules, here are the steps: Click the blue "Editorial Rules" to select the ACL, choose MAC type as shown in figure 8, choose IP type as shown in figure 9, click "Add" to enter the ACL Rules configuration page, as shown in figure 10. Access different configuration pages depending on the type of ACL selected. The MAC type is shown in figure 11 and the IP type is shown in figure 12.

CL		
Create Delete		
Name	Туре	Operation
ac1	mac	Editorial Rules
🔲 a1	ip	Editorial Rules
L Rules		
Current ACL Name:ac1 Type:mac(click	the [editorial rules] button in the access control operation bar to configure this.)	
Add Delete		
Sequence Number	ACL Entry	
	Figure 8 Select MAC type ACI	
	Figure 8 Select MAC type ACL	
Create	Figure 8 Select MAC type ACL	
Create Delete	Figure 8 Select MAC type ACL	Operation
Create Delete Name	Figure 8 Select MAC type ACL Type mac	Operation Editorial Rules
Create Delete Name ac1 acl2	Figure 8 Select MAC type ACL	Operation Editorial Rules Editorial Rules
Create Delete Name ac1 acl2 Rules	Figure 8 Select MAC type ACL	Operation Editorial Rules Editorial Rules
Create Delete Name ac1 ac12 acl2 Rules Type: (clicl)	Figure 8 Select MAC type ACL Type mac ip k the [Editorial Rules] button in the ACL operation bar to configure this.)	Operation Editorial Rules Editorial Rules
Create Delete Name ac1 ac1 ac2 Rules Type: (click Add Delete	Figure 8 Select MAC type ACL	Operation Editorial Rules Editorial Rules

Figure 9 Select IP type ACL

ACL Rules	
Current ACL Name: ac1	Type: mac(click the (Editorial Rules) button in the ACL operation bar to configure this.)
Add Delete	
Sequence Number	ACL Entry

Figure 10 Add ACL operation

Add Rule		
ccess List Name	acl	
ype	mac 👻	
equence Number	Please Enter	
rtion	Demit *	
urce Mac Address		
urce Mac Address Wildcard Mask	· · ·	
est Mac Address		
est Mac Address Wildcard Mask		
AN	Please Enter	(1-4094)
ntag VLAN	○ Enable	
s		
terior Vlan	Please Enter	(1-4054)
ner Cos	×	
otocol	÷	
	Submit Exit	

Figure 11 MAC ACL add rule

Parameter usage

Item	Description
Sequence Number	The serial number of the filter in the MAC ACL. If this field is not displayed, it can be generated automatically
Action	Select the action of mac ACE
Source Mac Address	Enter the source MAC address
Source Mac Address Mask	Enter the source MAC address wildcard bits
Dest Mac Address	Enter the destination MAC address



Inner Vlan	Enter Inner VLAN-ID, the range is 1 to 4094
Inner Cos	Enter Inner CoS, the range is 0 to 7
Protocol	Select the protocol type which including ARP, RARP or Ether type
Туре	Select the L2 type including ETH2, SNAP, SAP

CL Add Rule		
Access List Name	acl2	
Туре	ip	•
Sequence Number	Please Enter	(1~131071
Action	Permit	~
IP Protocol	ANY	•
Source IP Address		(0.0.0)
Source IP Address Wildcard Mask	e s s	(0.0.0.0)
Dest IP Address		(0.0.0)
Dest IP Address Wildcard Mask		(0.0.0)
DSCP	Please Enter	(0~63)
Routed		
Option		

Figure 12 IP ACL add rule



• Parameter usage

ltem	Description
Sequence Number	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented
Action	Select the action of IP ACE
IP Protocol	Select IP protocol of IP ACE
IP Protocol Num	Enter IP protocol number, the range is 0 to 255
Source IP Address	Enter the destination MAC address
Source IP Address Mask	Enter the destination MAC address wildcard bits
Dest IP Address	Enter VLAN-ID, the range is 1 to 4094
Dest IP Address Mask	Enter CoS, the range is 0 to 7
Source Port Type	Select source port type
Source Port Num	Enter source port number
Source Port Range	Enter source port range
Dest Port Type	Select destination port type
Dest Port Num	Enter destination port number
Dest Port Range	Enter destination port range
ІСМР Туре	Enter ICMP type, the range is 1 to 255
ICMP Code	Enter ICMP code, the range is 1 to 255
IGMP Type	Select IGMP type.
DSCP	Enter DSCP
Fragments	Select fragments
Routed	Select routed
option	Select option

The parameters that need to be configured are configured according to the actual requirements, the non-demanding parameters can be left unconfigured. If you want to configure ACL rules, perform the following steps:
(1) Enter VLAN in the "VLAN " text box.
(2) Select arp in the "Protocol " drop-down box.
(3) Click the submit to complete the configuration.

The operation is shown in figure 13, and ACL Rules is successfully configured as shown in figure 14.

C4 data A car la fume jegener Kunler Genera Kunl				
Acceded to the set of	KCL Add Rule			
Type Image:	Access List Name	act		
Separate Number Image Separate Number Anion Server Nuck Address Server N	Туре	mac	¥	
Action Source Nac Address Source Nac Address<	Sequence Number	Please Enter		
Saver Mac Address Windcard Mack Saver Mac Address Windcard Mack Det Mac Address Windcard Mack VAN 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Action	Permit	×	
Searce Mae Address Wildcard Mae Cest Mae Address Wildcard Mae Cest Mae Address Wildcard Mae Cos Cos Cos Cos Cos Cos Cos Co	Source Mac Address	n 12		
Det Mac Address Wildord Hatt Cet Mac Address Wildord Hatt Ann	Source Mac Address Wildcard Mask	C 9		
Det Mac Address Wildows Maker Strain	Dest Mac Address			
VLN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Dest Mac Address Wildcard Mask	s 9		
Uniteg VLAN COS Interior VLan Person of the memory o	VLAN 1	1	(1-4094)	
COS I I I I I I I I I I I I I I I I I I I	Untag VLAN	🔿 Enable 💿 Disable		
Inter Coc Protocol Compared to the form Protocol Compared	cos		×	
Inner Ces Pretocol 2 arp 3 codemi code Figure 13 Add ACL rules L Rules	Interior Vlan	Please Enter	(1-4094)	
Pressool 2 app * 3 Cool 6 of Figure 13 Add ACL rules	Inner Cos		v	
3 Com Con Figure 13 Add ACL rules	Protocol 2	arp	v.	
Figure 13 Add ACL rules	3	Submit Exit		
1. Rules			Figure 13 Add ACL rules	
	L Rules			

Figure 14 New ACL rules information

ACL Ent

If you want to delete the ACL rules, here are the steps: Click on the blue "Editorial Rules" to select the current ACL, as shown in figure 15.

Operation
Editorial Rules
Editorial Rules

Figure 15 Select current ACL

- If you want to delete the configuration, perform the following steps:(1) Click the checkbox to select ACL rules which are need to be deleted as the figure below.
- (2) (3) Click "Delete" button. After clicking "Delete", the page as shown in figure 16 appears, and if you click the "Confirm" button, you can delete it.

Access Control List Class Map Policy Map			
ACL			
Create Delete			
Name	tips	×	Operation
ac1	црэ 	_	Editorial Rules
acl2			Editorial Rules
ACL Rules	Are you sure to delete selected entry?		
Current ACL Name: ac1 Type: mac(click the [Editorial Rules] but 2 Add Delete	3 Confirm Cancel		
Sequence Number	ACL Entry		
1 💌 10	permit src-mac any dest-mac any protocol arp		

Figure 16 Delete ACL rules

16.2 Class Map

If you click "ACL -> Class Map" in the title bar, the class map page appears, as shown in figure 17.

FS 55800-8TF125		Monitor	Configuration	% Maintenance	Network	
		_				
🕑 Ethernet Status	Access Control List Class M	ap 2 Policy Map				
👳 Link Aggregation						
🐹 Storm Control	Class Map					
Flow Control	Create					
Port Isolate	Name		Туре			Operation
Port Detect						
11 VLAN						
BB VLAN Classifier				111		
🖵 MAC				No data-		
🛱 Spanning Tree						
4¢ ERPS						
I Mirror						
😤 Multicast						
🚇 QOS	Class Map Match ACL					
🗹 ACL 1	Class Map Name: Type: (lick the [Match] button in t	he Class Map operation of			
	Add Delete					
			Copyright (0 2009-2020 FS.COM Inc . /	All Rights Reserved.	

Figure 17 Class map page

16.2.1 Class map

Class map provide two basic configuration functions, creating and removing class map. If you want to create an class map, here are the steps: If you click the "Create" button, you can add class map, the operation is shown in figure 18, and then the class map configuration page appears, as shown in figure 19.

Class Map		
Create		
Name	Туре	Operation

Figure 18 Add class map operation

Create Class Map		
* Class Map Name	Please Enter	
* Туре	match any	٣
	Create	

Figure 19 Add class map

Parameter usage

Item	Description	
Class Map Name	Enter the class map name	
Туре	Select the class map type	

- If you want to configure class map, perform the following steps:
 (1) Enter class map name in the "class map name" text box..
 (2) Select the type of create class map in the "type " drop-down box.
 (3) After that, click Create to apply all the changes made.
- (4) Click "Create " button.
- Confirm the submission configuration and click the "Create " button. (5)

The operation is shown in figure 20, and the class map configuration success table entry is shown in figure 21.

e Class Map Ilass Map Name	1 at			
ype	2 match any	*		
	3 Create Exit	tips	×	
		Are you sure to	to configure?	
		4 Create	cancel	

Figure 20 Add class map configuration

Class Map		
Create Delete		
Name	Туре	Operation
🗋 a1	match-any	Match

Figure 21 New class map

If you want to delete the class map, here are the steps:

Click the checkbox to select class map which are need to be deleted as the figure below. (1)

- (2) Click "Delete" button.
- After clicking "Delete", the page as shown in figure 22 appears, and if you click the "Confirm" button, you can delete it. (3)

Access Control List Class Map Policy Map			
Class Map			
Create Delete 2			
□ Name	tips	×	Operation
1 🛛 at	riha.		Match
Class Map Match ACL			
Class Map Name: Type: (click the [Match] button in the Class N	Are you sure to delete selected Class Map?		
Add Delete			
Access List Name	Confirm Cancel		

Figure 22 Delete class map

16.2.2 Class Map Match ACL

Class map match ACL provide two basic configuration functions, creating and removing class map match ACL.

If you want to create an class map match ACL, here are the steps:

Click "Match" in blue to select the current class map matching ACL, as shown in figure 23, and click "Add" to enter the class map match ACL configuration page, as shown in figure 24, class map match ACL the configuration page is shown in figure 25.

Access Control List	Class Map Pol	y Map	
lass Map			
Create			
Name		Туре	Operation
🗌 a1		match-any	Match
lass Map Match ACL			
Class Map Name:	Type: (click the [Match]	utton in the Class Map operation column to configure this.)	
Add Delete			
Access List Name		Туре	
		11	
		No data-	
		Figure 23 Select curr	rent class map
		-	
Class Map Match ACL			
Class Map Name: a1	Type: match-any(clic	the [Match] button in the Class Map operation column to co	
Add Delete			
Access List Name		Туре	
		1	
		No data~	
		Copyright © 2009-2020 FS.COM Inc	c . All Rights Reserved.
		F : 24A I I I	

s map match Act		
lass Map Name: al Type: match-any		
Submit Exit		
Name Name	Туре	

Figure 25 Class map match ACL configuration page

Parameter usage

Item	Description
Name	acl name
Туре	acl type

If you want to configure class map match ACL, perform the following steps:

Click the checkbox to select ACL which are need to be matched to the current Class map. (1)

- (2) Click "Submit " button.

(3) Confirm the submission configuration and click the "Submit " button.
 The operation is shown in figure 26, the class map match ACL configuration success table entry is shown in figure 27.

Access Control List Class Map Policy Map		
Class Map Match ACL Class Map Name: qwe Type: match-any		
2 Submit Exit	tips	×
ac1		
1 🗷 acl2	Are you sure to add selected ACL?	
	3 Submit cancel	

Figure 26 Class map match ACL configuration

Class Map Match ACL Class Map Name: a1 Add Delete	Type: match-any(click: the [Match] button in the Class Map operation column to configure this.)
Access List Name	Туре
🗋 ac1	match-any

Figure 27 New class map match ACL

If you want to delete the class map match ACL, here are the steps: Click on the blue "Match" and select the current Class map, as shown in figure 28.

Class Map		
Create Delete		
Name	Туре	Operation
🗌 a1	match-any	Match
Class Map Match ACL		
Class Map Name: a1	Type: match-any(click the [Match] button in the Class Map operation column to configure this.)	
Add Delete		
Access List Name	Туре	
ac1	match-any	

Figure 28 Select current Class map

If you want to delete the configuration, perform the following steps:

- (1) Click the checkbox to select class map match ACL which are need to be deleted as the figure below.
- (2) Click "Delete" button.
- (3) After clicking "Delete", the page as shown in figure 29 appears, and if you click the "Confirm" button, you can delete it.

Create Delete			
Name	tips	×	Operation
lass Map Match ACL Class Map Name; a1 Type: match-any(click the [Match] button	Are you sure to delete selected entry?		Wakch
Add Delete 2	3 Confirm Cancel		
R act	match-any		

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Figure 29 Delete class map match ACL

16.3 Policy Map

If you click "ACL -> Policy Map" in the title bar , the Policy Map page appears, as shown in Figure 30.
FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network	
			2			
Ethernet Status	Access Control List Class Map	Policy Map	-			
🕸 Link Aggregation	Policy Map					
X Storm Control						
[1] Flow Control	Create					
Port Isolate	Policy Map Name					Operation
Port Detect						
님 VLAN						
BB VLAN Classifier				1		
MAC MAC				No data-		
🗄 Spanning Tree						
d₀ ERPS						
I Mirror						
${}_{\delta}^{\mathcal{G}}{}_{\delta}$ Multicast	and can't strengthered as					
a qos	Policy Map Match Class Map					
Z ACL 1	Class Map List in Policy Map: (click the [M	atch] button in the P	olicy Map operation colu			

Figure 30 Policy map

16.3.1 Policy Map

Policy map provide two basic configuration functions, creating and removing policy map. If you want to create an policy map, here are the steps:

If you click the "Create" button, you can add the policy map, the operation is shown in Figure 31, and then the policy map configuration page appears, as shown in Figure 32.

Create	
Policy Map Name	Operation
	No data~
F	igure 31 Add policy map operation
Create Policy Map	
* Policy Map Name Please Enter	
Create Eat	
	Figure 32 Add policy map
rameter usage	
Item	Description
Policy Map Name	Enter the policy map name
I want to configure policy map, perform the foll- Enter name in the "policy map name" text box	owing steps:
After that, click Create to "Create" all the change	jes made.

(4) Confirm the submission configuration and click the "Create " button.

The operation is shown in figure 33, and the policy map configuration success table entry is shown in figure 34.

Create Policy Map * Policy Map Name a7 2 Create Est			
	tips	×	
	Are you st	ure to configure?	
	Figure 33 Add polic	y map configuration	
Policy Map Create Delete			

Policy Map Name	Operation
□ a7	Match

Figure 34 New policy map

If you want to delete the policy map, here are the steps:

- (1) Click the checkbox to select policy map which are need to be deleted as the figure below.
- (2) Click "Delete" button.
- (3) After clicking "Delete", the page as shown in figure 35 appears, and if you click the "Confirm" button, you can delete it.

Create Delete 2			
Policy Map Name	time	~	Operation
1 🔽 a7	ups	_	Match
Policy Map Match Class Map Class Map List in Policy Map: a7(click the [Match] button in the Policy MA	Are you sure to delete selected Policy Map?		
Add Delete	3 Confirm Cancel		Operation

Figure 35 Delete policy map

16.3.2 Policy Map Match Class Map

Policy map match class map provides two basic configuration functions, namely creating and deleting policy map match class map. If you want to create an policy map match class map, here are the steps:

Click the blue "Matching" to select the current strategy classification, as shown in figure 36, click "Add" to enter the policy map match class map configuration page, as shown in figure 37, policy map match class map configuration page is shown in figure 38.

Policy Map	
Create	
Policy Map Name	Operation
D #7	Match
Policy Map Match Class Map	
Class Map List in Policy Map: a7[click the [Match] button in the Policy Map operation column to configure this.)	
Add Delete	
Class Map Name	Operation
38.	
No data-	
Policy Map Apply Interface	
Interface service with Policy Mag: a7(click the (Match) button in the Policy Map operation column to configure this.)	
Add Ooleter	
Figure 36 Select policy map	
· · · · · · · · · · · · · · · · · · ·	
olicy Map Match Class Map	
Class Map List in Policy Map: (click the [Match] button in the Policy Map operation column to configure this.)	
Add Delete	
Class Map Name	Operation
Figure 37 Add button	

Policy Map Name: a7			
 Class Map Name 	class-default	*	
- Policer	Policer	v .	
- Color Mode	color blind	٠	
Policer Mode	RFC2697	٠	
- CIR	Please Enter CIR		(8-10
CBS	Please Enter CBS		
EBS	Please Enter		
Drop Color	Red	w.	
Redirect To		٣	
Monitor		*	

Figure 38 Policy map match class map configuration page

• Parameter usage

ltem	Description		
Class Map Name	Select the existed class map		
Policer	Select the peolicer or not		
Color Mode	Select the color mode		
Policer Mode	Select the policer mode		
CIR	Enter CIR (Commit Information Rate) with the range of 1 to 10,000,000 kbps		

ltem	Description		
CBS	Enter CBS(Commit Burst Size) with the range of 0 to 16,000 bytes		
EBS	Enter EBS(Excess Burst Size) with the range of 0 to 16,000 bytes		
PIR	Enter PIR(Peak Information Rate) with the range of 1 to 10,000,000 kbps		
PBS	Enter PBS (Peak Burst Size) with the range of 0 to 16,000 bytes		
Drop color	Select the drop color		
Redirect to	Select the redirection interface		
Monitor	Select the monitor session		

If you want to configure an policy map match class map, here are the steps:

- (1) Select name in the "class map name" drop-down box.
- (2) Select no police in the "Policer" drop-down box.
- (3) Click the "submit" to complete the configuration, as shown in the figure 39.
- (4) Click "Submit " button.

The operation is shown in figure 39.

lass Map Name	class-default	*	
Policer 2	No Policer	v	
direct To		* tips X	
onitor		*	
3	Submit Exit	Are you sure to configure?	
		4 cancel	

Figure 39 Configuration example

If you want to view the configuration, follow these steps:

(1) Click "Particulars" to view the detailed configuration, the operation process is shown in figure 40, the detailed configuration is shown in figure 41.



If you want to delete the policy map match class map, here are the steps:

Click the blue "Match" to select the current Strategy classification, as shown in the figure 42.

Policy Map		
Create Delete		
Policy Map Name		Operation
🗌 a7		Match
olicy Map Match Class Map		
Class Map List in Policy Map: a7(click the [Match]	button in the Policy Map operation column to configure this.)	
Add Delete		
Class Map Name		Operation
Class-default		Particulars
olicy Map Apply Interface		
Interface service with Policy Map: a7(click the [Ma	tch] button in the Policy Map operation column to configure this.)	
Add Delete		
Interface Name	Direction	

Figure 42 Select policy map

If you want to delete the configuration, perform the following steps:

- (1) Click the checkbox to select policy map match class map which are need to be deleted as the figure below.
- (2) Click "Delete" button.
- (3) After clicking "Delete", the page as shown in figure 43 appears, and if you click the "Confirm" button, you can delete it.

Policy Map			
Create Delete			
Policy Map Name			Operation
_ a7			Match
Policy Map Match Class Map			
Class Map List in Policy Map: a7(click the [Match] button in the Policy Me Add Delete 2	tips	×	
Class Map Name	Are you sure to delete selected Class Map?		Operation
1 Zass-default			Particulars
Policy Map Apply Interface	3 Confirm Cancel		
Interface service with Policy Map: a7(click the [Match] button in the Policy Add Delete	Map operation column to configure this.)		
Interface Name	Direction		

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Figure 43 Delete policy map match class map

16.3.3 Policy Map Apply Interface

Policy map apply interface provide two basic configuration functions, creating and removing policy map apply interface.

If you want to create an policy map apply interface, here are the steps:

Click "Match" in blue to select the current policy category, as shown in figure 44, click "Add" to go to the policy map apply interface configuration page, as shown in figure 45, and the class map list in the policy map apply interface configuration page is shown in figure 46.

Access Control List	Class Map	Policy Map					
aliar Man							
Create							
Cicale							
Policy Map Name	2						Operation
							Match
Olicy Map Match Class	s Map	hī button in the Policy N					
Add Delete	map. ar tener the finate						
Class Map Name							Operation
Class-derault							Particulars
olicy Map Apply Inter	face		P				
Interface service with P	olicy Map: a/(click the [r						
Add							
Interface Name			Direction				
			Copyright © 2009-2	2020 FS.COM Inc . All Ri	ghts Reserved.		
			F :	4.4. Calaat aa li			
			Figure 4	44 Select polic	у тар		
v Map Apply Interface							
erface service with Policy Map:	a7(click the [Match] button in	the Policy Map operation col	lumn to configure thic)				
Add Delete							
Interface Name			Direction				
		Figur	re 45 Add polic	y map apply i	nterface op	peration	
olicy Map Ap	oply Interfa	ce					
D [] 14	-						
Policy Map	Name: a/						

THE THE THE THETTE	In	ter	fac	e N	Va	m	e
--------------------	----	-----	-----	-----	----	---	---

Direction

Inout	
Input	

Figure 46 Policy map apply interface configuration page

Parameter usage

ltem	Description
Interface Name	Select the interface name
Direction	Select the direction

If you want to check the configuration policy map apply interface, please perform the following steps:

- (1) Select the interface in the "Interface Name" drop-down box.
- (2) Select direction in the "Direction" drop-down box.
- (3) After that, click "Submit " to complete the configuration.

The operation is shown in figure 47, the policy map apply interface configuration success table entry is shown in figure 48.

Policy Map Apply Inter	rface		
Policy Map Name: a7			
Interface Name	eth-0-1	-	
Direction	Input	▼ 2	
	3 Submit Exit		

Figure 47 Add policy map apply interface operation

nterface service with Policy Map: a7(click the [Match] button in the Policy Map operation column to configure this.)						
Add Delete						
Interface Name	Direction					
□ eth-0-1	input					

Figure 48 View policy map apply interface

If you want to delete the policy map apply interface, here are the steps: Click the blue "Match" to select the current Strategy classification, as shown in the figure 49.

Access Control List	Class Map	Policy Map	
Policy Map			
Create Delete			
Policy Map Name			Operation
🗌 a7			Match
Policy Map Match Class	Мар		
Class Map List in Policy	Map: a7(click the [Mat] button in the Policy Map operation column to configure this.)	
Add Delete			
Class Map Name			Operation
🗹 class-default			Particulars
Policy Map Apply Interf	ace		
Interface service with Po	olicy Map: a7(click the	latch] button in the Policy Map operation column to configure this.)	
Add Delete			
Interface Name		Direction	
		Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.	

Figure 49 Select policy map

If you want to delete the configuration, perform the following steps:

- (1)
- (2) (3)
- Click the checkbox to select policy map apply interface which are need to be deleted as the figure below. Click "Delete" button. After clicking "Delete", the page as shown in figure 50 appears, and if you click the "Confirm" button, you can delete it.

Policy Map Match Class Map Class Map List in Policy Map: <mark>a7</mark> (click the [Match] button in the Policy Mi	tips ×	
Add Delete	Are you sure to delete selected Interface?	
Class Map Name		Op
Class-default	3 Confirm Cancel	Par
Policy Map Apply Interface		
Interface service with Policy Map: a7(click the [Match] button in the Policy	Map operation column to configure this.)	
Add Delete 2		
Interface Name	Direction	
1 eth-0-1	input	

Copyright © 2009-2020 FS.COM Inc . All Rights Reserved.

Figure 50 Delete policy map apply interface

17. Reboot/Save

If you want to restart the switch or save the current configuration under the web page, you should click "Maintenance" in the top control bar. Then click "Reboot/Save" in the navigation bar, the correspond page appears.

17.1 Page Overview

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network	Save admin Logou
Reboot/Save 2 System Configuration	Save configuration to startup-config — Save configuration to startup-config		Save	1		
E Load Configuration	Reboot the switch					
File Management	Reboot the switch		Save system configuration be	efore reboot		
Log Management			Reboot			
SNMP						
SNMP Trap	Restore factory configuration to startup-co	infig				
1 Worm Intercept	Restore factory configuration to startup-co	infig	Recovery			
Ø DDoS Intercept						
ARP Intercept						
Currently Sessions						
A User Management						

Figure 1 Reboot/Save page

Parameter usage

ltem	Description
Save configuration to startup-config	Save current configuration to startup-config
Save system configuration before reboot	Save current configuration to startup-config before reboot
Restore Factory configuration to startup-config	Restore switch by using startup-config

17.2 Save Configuration

Click "Save" button to save current configuration to startup-config.



Figure 2 Save config

17.3 Reboot Switch

Click "Reboot" button to reboot the switch, but if you want to save the current configuration before reboot, choose "Save system configuration before reboot" at first.



Figure 3 Reboot switch

17.4 Recovery Switch

 ${\it Click} \ \ "Recovery" \ \ button to recovery switch \ configuration \ with \ startup-config.$

Restore factory configuration to startup-config

Restore factory configuration to startup-config



Figure 4 Recovery switch

18. System Configuration

If you click "Maintenance -> System Configuration" in the top control bar, the System Configuration list page appears, as shown in figure 1.

FS 55800-87F125		Monitor	Configuration	Maintenance	Network	Save admin Logou
C Reboot/Save System Configuration C Load Configuration C File Management C Log Management SNMP SNMP SNMP Worm Intercept	Base Settings Management IP MASK Gateway Thermal Sensor	192 . 168 . 255.255.255.0(24) 0 , 0 . Apply	. 1 . 1	1	default 67630 unit exerciseste	
DDoS Intercept ARP Intercept	THUTTHU JULIAN	Apply				
Currently Sessions	Base Information					
R User Management	Device Name	\$5800-8TF125-119			(1-63 chars)	
	Contact	Please enter			(1255 chars)	
	Location	Please enter			(1~255 chars)	
		Figu	Copyright re 1 System d	o 2009-2020 rs.com	M Inc. All Rights Reserved.	

18.1 Base Settings

After you click "System Configuration" button, you will see the first case "base settings". If you want to add the IP for this switch, you can follow the following steps:

- (1) Enter an IP address in the "Management IP.
- (2) Select the destination address mask in the "mask " dropdown box.
- (3) Enter default route IP address in the "Gate Way" textbox.
- (4) Click "Apply" button, and a tips popup will appear, as shown in figure 2 and figure 3, then click "Apply" button in tips.

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network	Save admin Logout
	Race Settings					
🔿 Reboot/Save	Management ID					
System Configuration	management	192 . 168	. 1 . 1			
E Load Configuration	MASK	255.255.255.0(24)		*		
🖹 File Management	Gateway	0 0	. 0 0			
Log Management						
I SNMP		Apply				
SNMP Trap	Thermal Sensor					
10 Worm Intercept	Thermal Sensor	5	75	90	lefault: 5/75/90 , unit: centigrade	
Ø DDoS Intercept						
ARP Intercept		Apply				
💬 Currently Sessions	Base Information					
୍	Device Name	\$5800-8TF125-119			(1-63 chars)	
	Contact	Please enter			(1–255 chars)	
	Location	Please enter			(1-255 chars)	
			Copyright	t © 2009-2020 FS.COM	Inc . All Rights Reserved.	

(5 Reboot/Save	Base Settings				
System Configuration	Management IP	192 . 168 . 1	. 1		
E Load Configuration	MASK	255.255.255.0(24)	*		
File Management	Gateway	0 0 0	0		
🖹 Log Management			tips	×	
SNMP		Apply			
SNMP Trap	Thermal Sensor				
🗓 Worm Intercept	Thermal Sensor	5 75	Setting management ip reconnect, continue?	address need	ade
Ø DDoS Intercept					
ARP Intercept		Apply	Apply	Cancel	
Currently Sessions	Base Information				
P, User Management	Device Name	S5800-8TF12S-119		(1-63 chars)	
	Contact	Please enter		(1-255 chars)	
	Location	Please enter		(1~255 chars)	
			Copyright © 2009-2020 FS.CO	M Inc . All Rights Reserved.	

Figure 3 Base settings page

• Parameter usage

ltem	Description
Management IP	Manage switch via this IP
Mask	Locate Management IP's network bits
Gate Way	Defaults route

18.2 Thermal Sensor

After you click "System Configuration" button, you will see the second case "thermal sensor" in this case you can set the threshold of temperature. The boxes from left to right represent the definition of low temperature, medium temperature, and high temperature.

Sensor				
1 9611901	D	75	90	default: 5/75/90 , unit: centigrad

Figure 4 Termal sensor

Notes: From left to right in the table are the low threshold middle threshold and high threshold of the set temperature.

18.3 Base Information

After you click "System Configuration" button, you will see the third case "Base Information", in this case you can set the switch information to distinguish the switch in network.

Device Name	DUT1	(1~63 chars)
Contact	Please enter	(1~255 chars
Location	Please enter	(1~255 chars

Figure 5 Base information

• Parameter usage

ltem	Description
Device Name	Switch hostname
Contact	How to contact this switch in the other words contact is manage IP of this switch or Other information which can visit this switch
Location	Where the switch is

If you want to set the information of this switch, you can follow the following steps:

- (1)
- (2)
- Enter an device name in the "Management IP. Enter contact information in the "Contact" Enter location information in the "Location" textbox. (3)
- Click the Apply button. (4)

18.4 Date&Time

After you click "System Configuration" button, you will see the fourth case "Date and Time" in this case you can set time of switch.

Date and Time		
Date and Time	16:23:05 06/15/2020	(HH:MM:SS MM/DD/YYYY)
	Apply	
	Figure 6 Date and time	

Example: 12:08:44 17/03/2020

18.5 Time Zone Name

After you click "System Configuration" button, you will see the 5th case "Time Zone Name" in this case you can set the time zone and the offset of time zone.

UTC									(3~32 chars)
add 💌	0		hour	0		min	0		sec
	UTC	UTC	UTC add 💌 0 💌	UTC add 💌 0 💌 hour	UTC add v 0 v hour 0	UTC add v 0 v hour 0 v	UTC add v 0 v hour 0 v min	UTC add v 0 v hour 0 v min 0	UTC add v 0 v hour 0 v min 0 v

Figure 7 Time zone name

• Parameter usage

ltem	Description
Time Zone Name	Time zon e
Offset	Offset depends between GMT and Time Zone which your set

If you want to set the time zone name of this switch, you can follow the following steps:
(1) Enter time zone name in the "Time Zone Name.
(2) Select the offset in the "Offset".

19. Load Configuration

If you click "Maintenance > Load Configuration" in the top control bar, the load configuration list page appears, as shown in figure 1.

FS 55800-8TF12S		Monitor	Configuration	Maintenance	Network	Save admin Logout
 Reboot/Save System Configuration 	Load Configuration			1		
E Load Configuration 2	Filename		Time		Size	Operation
File Management	flash:/startup-config.conf		2020-06-20 01	21:24	2.4K	Download
🖹 Log Management	○ flash:/startup-config.conf.200517.0		2020-05-17 06	:06:28	3.0K	Download
SNMP	○ flash:/startup-config.conf.200517.1		2020-05-17 08	24:19	3.0K	Download
SNMP Trap	 flash:/startup-config.conf.200517.2 		2020-05-17 08	28:04	3.0K	Download
🖄 Worm Intercept	 flash:/startup-config.conf.200525.0 		2020-05-25 22	30:57	8.8K	Download
Ø DDoS Intercept	○ flash:/startup-config.conf.200525.1		2020-05-25 22	:40:02	8.8K	Download
ARP Intercept	flash:/startup-config.conf.200525.2		2020-05-25 22	40:12	8.8K	Download
Currently Sessions	 flash:/startup-config.conf.200525.3 		2020-05-25 22	:40:20	8.8K	Download
A User Management	 flash:/startup-config.conf.200525.4 		2020-05-25 22	40:29	8.8K	Download
	flash:/startup-config.conf.200607.0		2020-06-07 02	:33:17	1.7K	Download

Figure 1 Load configuration list

This chapter describes load the configuration files to the device or download the configuration file to PC as the the backup file.

19.1 Load Configuration

You can load the configuration files from the web to the device and replace the configuration file that is currently being used.

19.1.1 Load the Configuration Files

If you want to load the configuration files to replace the configuration file that is currently being used, you can follow the following steps : (1) Choose a configuration file which through the file name.

(2) Click "Load" button.

(3) It will appear tips page to note you to confirm the operation, if you click "Loading" button, it will use the configuration as the new configuration of device; if you click "cancel" button, you will cancel the loading configuration operation.

The operation is shown in figure 2.

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network		Save admin Logout
 Reboot/Save System Configuration 	Load Configuration						
Load Configuration	Filename		Time			Size	Operation
E File Management	1 flash:/startup-config.conf		2020-06-20 01:	21:24		2.4K	Download
Log Management			² tips		×	3.0K	Download
I SNMP	 flash:/startup-config.conf.200517.1 		2			3.0K	Download
SNMP Trap	○ flash:/startup-config.conf.200517.2		2			3.0K	Download
🖄 Worm Intercept	flash:/startup-config.conf.200525.0		2	onfirm that you want to lo	ad the selected file?	3.8K	Download
⊘ DDoS Intercept	flash:/startup-config.conf.200525.1		2			3.8K	Download
ARP Intercept	flash:/startup-config.conf.200525.2		2 3	Loading	cancel	3.8K	Download
💬 Currently Sessions	flash:/startup-config.conf.200525.3		2020-05-25 22:	40:20		8.8K	Download
A User Management	 flash:/startup-config.conf.200525.4 		2020-05-25 22;	40:29		8.8K	Download
	○ flash:/startup-config.conf.200607.0		2020-06-07 02:	33:17		1.7K	Download

Figure 2 Load configuration operation

Parameter usage

ltem	Description
Filename	Display name of configuration file



Time	Display last modified time of configuration file
Size	Display size of configuration file
Operation	Display that the configuration file can be downloaded

19.1.2 Refresh the Load Configuration Page

If you want to refresh the load configuration page, you can click "Refresh" button. The operation is as shown in Figure 3.

Load Configuration			
Load Refresh			
Filename	Time	Size	Operation
○ flash:/startup-config.conf	2020-06-20 01:21:24	2.4K	Download
○ flash:/startup-config.conf.200517.0	2020-05-17 06:06:28	3.0K	Download
○ flash:/startup-config.conf.200517.1	2020-05-17 08:24:19	3.0K	Download
) flash:/startup-config.conf.200517.2	2020-05-17 08:28:04	3.0К	Download
) flash:/startup-config.conf.200525.0	2020-05-25 22:30:57	8.8K	Download
) flash:/startup-config.conf.200525.1	2020-05-25 22:40:02	8.8K	Download
○ flash:/startup-config.conf.200525.2	2020-05-25 22:40:12	8.8K	Download
O flash:/startup-config.conf.200525.3	2020-05-25 22:40:20	8.8K	Download
O flash:/startup-config.conf.200525.4	2020-05-25 22:40:29	8.8K	Download
○ flash:/startup-config.conf.200607.0	2020-06-07 02:33:17	1.7K	Download

Figure 3 Refresh the load configuration information

19.1.3 Download the Configuration Files

You can download the configuration file and saved in the disk of PC or in the mobile storage device as the backup file and you can also see the configuration file.

To download the configuration file, you can select the configuration file you want to download, and click "Download" button to save the file, the operation is as shown in Figure 4.

Load Configuration			
Load			
Filename	Time	Size	Operation
○ flash:/startup-config.conf	2020-06-20 01:21:24	2.4K	Download
○ flash:/startup-config.conf.200517.0	2020-05-17 06:06:28	3.0К	Download
○ flash:/startup-config.conf.200517.1	2020-05-17 08:24:19	3.0К	Download
○ flash:/startup-config.conf.200517.2	2020-05-17 08:28:04	3.0К	Download
○ flash:/startup-config.conf.200525.0	2020-05-25 22:30:57	8.8K	Download
○ flash:/startup-config.conf.200525.1	2020-05-25 22:40:02	8.8K	Download
○ flash:/startup-config.conf.200525.2	2020-05-25 22:40:12	8.8K	Download
○ flash:/startup-config.conf.200525.3	2020-05-25 22:40:20	8.8K	Download
○ flash:/startup-config.conf.200525.4	2020-05-25 22:40:29	8.8K	Download
○ flash:/startup-config.conf.200607.0	2020-06-07 02:33:17	1.7K	Download

Figure 4 Download configuration file operation

20. File Management

If you click "Maintenance -> File Management" in the top control bar, the file management page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network		Save admin Logout
() Reboot/Save	Memory Usage			1			
System Configuration Load Configuration File Management	\sim	flash: Total size: 1.6G, Free size: 1.4G		flash:/boot Total size: 59.3M, I	Free size: 13.0M		
Log Management SNMP	File Management						
 SNMP Trap Worm Intercept 	Browse file	Please select the file to upload Upload As File Upload As Ima	Browse	file (The max size of	f file can be uploaded is 30M)		
 DDoS Intercept ARP Intercept 	Delete Selected	d Files					
Currently Sessions	Select Name		Directory		Size	Usage	Operation
R User Management	web_qos_po	licer.cs Download	flash:		90.5K		
	webImage-	s350-5.5-en.bin Download	flash:		4.7M		
	startup-con	fig.conf Download	flash:		2.4K	Startup config*	Backup Config
	centecOS-e	350-8ts12x-v5.3.11.6.r.bin Download	flash:/boot		22.3M	System Image*	
			Copyright (C) 2009-2020 FS.COM I	nc . All Rights Reserved.		

Figure 1 File management

20.1 Memory Usage

Click "Maintenance > File Management" to check memory usage on switch, as shown in figure 2.

Memory Usage			
	flash: Total size: 1.6G, Free size: 1.5G	flash:/boot Total size: 59.3M, Free size: 13.1M	

Figure 2 Memory usage

• Parameter usage

ltem	Description					
flash:	Flash directory at the root of system					
flash:/boot	Flash:/boot directory at the root of system					

20.2 File Management

Click "Maintenance > File Management" to download or delete system and configuration files of switch, or upload files to switch, the configuration page is as shown in figure 4.

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network	Save admin Logout
() Reboot/Save	Memory Usage			1		
 System Configuration Load Configuration File Management 2 	flash: Total size: 1.6G, Free	e size: 1.5G		flash:/boot Total size: 59.3M, Fre	e size: 13.1M	
 Log Management SNMP 	File Management					

Figure 3 File management

e Management					
* Browse file	Please select the file to upload Upload As File Upload As Image	Browse file (The max size	e of file can be uploaded is 30M)		
Delete Select	ted Files				
Select Name		Directory	Size	Usage	Operation
web_qos	s_policer.cs Download	flash:	90.5K		
weblmag	ge-e350-5.5-en.bin Download	flash:	4.7M		
startup-	config.conf Download	flash:	2.4K	Startup config*	Backup Confi
centecO	DS-e350-8ts12x-v5.3.11.6.r.bin Download	flash:/boot	22.3M	System Image*	
centecO	0S.e350.8ts12x-4.0.r.bin Download	flash:/boot	22.3M	System Image	Use Image
power.lc	og Download	flash:/cold	1.5K	Cold log	
bhm.log) Download	flash:/cold	OB	Cold log	
diaglog	Download	flash:/info	4.9K		
web_arp	o.cs Download	flash:	8.4K		
web_inter	erface_mod.cs Download	flash:	32.8K		
Total 97 records.				10 💌 4 1 2 3	10 🕨 🔿

Figure 4 File management

• Parameter usage

ltem	Description
File List	File list: shows all files saved on current switch Name: system filename Directory: location of system files Size: size of system files in bytes Usage: description of system files Operation: operation for the special files , include: Use Image: use this file as the next boot image Backup Config: Save running configuration to this file Use Config: use this file as the next start up configuration
Upload As File	Upload the chosen files to Switch
Upload As Image	Upload the chosen files to Switch as a boot image
Delete Selected Files	Select files and delete them from Switch

NOTE: To download a file, just click the name of the file.

If you want to upload file/image/web image , please click "Browse File" button to select the file you need to upload, then click "Upload As File/Upload As Image/Upload Web Image" button, the operation is shown in figure 5.



FS 55800-8TF125		Monitor	Configuration	Maintenance	Network		Save admin Logout
	Marrieller						
() Reboot/Save	Memory Usage						
System Configuration							
E Load Configuration	flash:			flash:/boot			
E File Management	Total size: 1.60	i, Free size: 1.4G	~	Total size: 59.3M, Fre	e size: 13.0M		
Log Management							
SNMP	File Management						
SNMP Trap	* Browse file Please sele	ct the file to upload	Browse	file 1 (The max size of fi	le can be uploaded is 30M)		
③ Worm Intercept	Unload A	s File Upload As Ima	upload Web I	mage 2			
ODoS Intercept							
ARP Intercept	Delete Selected Files						
🗇 Currently Sessions	Select Name		Directory		Size	Usage	Operation
R User Management	web_gos_policer.cs Downlo	ad	flash:		90.5K		
	webImage-e350-5.5-en.bin	Download	flash:		4.7M		
	startup-config.conf Downk	oad	flash:		2.4K	Startup config*	Backup Config
	centecOS-e350-8ts12x-v5.	3.11.6.r.bin Download	flash:/boot		22.3M	System Image*	

Figure 5 Upload file configuration

If you want to delete files, you can select one or more file check box, click "Delete Selected Files" button to delete the file on switch, the operation is shown in figure 6.

Delete Selected Files				
Select Name	Directory	Size	Usage	Operation
web_qos_policer.cs Download	flash:	90.5K		
webImage-e350-5.5-en.bin Download	fi tips	×		
startup-config.conf Download	fl		Startup config*	Backup Config
centecOS-e350-8ts12x-v5.3.11.6.r.bin Download	fl		System Image*	
centecOS.e350.8ts12x-4.0.r.bin Download	fl Confirm	to delete the selected file or directory?	System Image	Use Image
power.log Download	fl		Cold log	
1 🛃 bhm.log Download	fl 3	Confirm	Cold log	
diaglog Download	flash:/info	4.9K		
web_arp.cs Download	flash:	8.4K		
web_interface_mod.cs Download	flash:	32.8K		
Total 97 records.			10 💌 📢 1 2 3 10	> >

Figure 6 Delete file configuration

If you want to download files, you can click the download button next to the file name to download, the operation is shown in figure 7.

FS SSB00-BTF12S		Monitor	Configuration	X Maintenance	Network		Save admin	Logout
	Memory Usage							
(J Reboot/Save								
System Configuration		flash:		flash:/boot				
E Load Configuration		Total size: 1.6G, Free size: 1.4G		Total size: 59.3M, Fre	e size: 13.0M			
E File Management								
Log Management	File Management							
E SNMP	* Browse file	Please select the file to upload	Browse fil	e (The max size of fi				
SNMP Trap								
🔅 Worm Intercept		Upload As File Upload As Imag	Upload Web Ima	ge				
Ø DDoS Intercept	Delete Selected	Files						
I ARP Intercept								
Currently Sessions	Select Name		Directory		Size	Usage	Op	eration
R User Management	web_qos_po	licer.cs Download	flash:		90.5K			
	webImage-e	350-5.5-en.bin Download	flash:		4.7M			
	startup-conf	fig.conf Download	flash:		2.4K	Startup config*	Bac	kup Config

Figure 7 Download file configuration

21. Log Management

If you click "Management->Log Management" in the top control bar, the log management page appears, as shown in figure 1.

FS E580-48X6Q		Monitor	Configuration	X Maintenance	Network		Save fs Logout
Reboot/Save System Configuration Load Configuration	Log Management		 Module All 	1		Search	
File Management	Refresh Clear	Module		Level		Content	
E Log Management 2	2006-04-18T19:49:54+08:00	IMI		4		Too many users.	
SNMP Trap	2006-04-18T19:47:06+08:00	IMI		4		Too many users.	
1 Worm Intercept	2006-04-18T19:47:04+08:00	IMI		6		Web user login, username fs, ip address 220.170.50.70	
Ø DDoS Intercept	2006-04-18T19:44:50+08:00	DHCLIENT		3		Interface vlan1 received No DHCPOFFER	
I ARP Intercept	2006-04-18T19:38:23+08:00	DHCLIENT		3		Interface vian1 received No DHCPOFFER	
💬 Currently Sessions	2006-04-18T19:33:36+08:00	IMI		4		Too many users.	
A User Management	2006-04-18T19:33:34+08:00	IMI		6		Web user login, username fs, ip address 59.63.203.138	
	2006-04-18T19:30:07+08:00	DHCLIENT		3		Interface vlan1 received No DHCPOFFER	
	2006-04-18T19:24:04+08:00	DHCLIENT		3		Interface vlan1 received No DHCPOFFER	
	2006-04-18T19:19:40+08:00	DHCLIENT		3		Interface vlan1 received No DHCPOFFER	
	Total 300 records.					10 🔻 4 1 2 3	
			Соруг	right © 2019 by FS.COM All R	lights Reserved.		

Figure 1 Log management page

This section mainly describes how to search and view log information.

•	Parameter	usage
---	-----------	-------

ltem	Description			
Level	Display special log level as condition for search			
Module	Display special module creating logs as condition for search			
Time	Display the time of log generated			
Module	Display Name of the module generating the log			
Level	Display Log information level			
Content	Display The log content			

21.1 Search Log Management

21.1.1 Search Log Information by Level

If you want to search log information for a specified level, you can select the level of the log in the "Level" drop-down box, then click the "Search" button, the operation is shown in figure 2, and the search results are shown in figure 3.

Log	lanagement		
Leve	4-warning	• 1 Module All	v Search 2



Log Management				
Level 4-warning		Module All	• Search	
Refresh Clear				
Time	Module	Level	Content	
2006-04-18T20:20:52+08:00	IMI	4	Too many users.	
2006-04-18T19:49:54+08:00	IMI	4	Too many users.	
2006-04-18T19:47:06+08:00	IMI	4	Too many users.	
2006-04-18T19:33:36+08:00	IMI	4	Too many users.	
2006-04-18T19:11:21+08:00	IMI	4	Too many users.	
2006-04-18T19:04:20+08:00	IMI	4	Too many users.	
2006-04-18T17:53:59+08:00	IMI	4	Too many users.	
2006-04-18T17:41:51+08:00	IMI	4	Too many users.	
Total 300 records.			10 💌 🖣	1 2 3 30

Figure 3 Search results list

21.1.2 Search Log Information by Module

If you want to search log information for a specified module, you can select the module of the log in the "Module" drop-down box, then click the "Search" button, the operation is shown in figure 4, and the search results are shown in figure 5.

Log Management				
Level All		▼ 1 Module DHCLIENT ▼ Sea		
Log Management	Figure	e 4 Search log informati	on by module operation	
Level All	×	Module DHCLIENT	• Search	
Refresh Clear				
Time	Module	Level	Content	
2006-04-18T21:13:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T21:05:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T21:01:20+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:54:58+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:47:13+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:41:04+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:33:31+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:27:43+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:22:21+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
2006-04-18T20:16:12+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER	
Total 300 records.			10 💌 📢 1 2 3 - 30 🕨 🔶	

Figure 5 Search results list

21.2 Refresh Log Information

If you want to refresh the logs displayed in the table, you can click "Refresh" button, the operation is shown in figure 6, then the latest log information will be displayed, as shown in figure 7.

Clear			
Time	Module	Level	Content
2006-04-18T21:19:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:13:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:11:28+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.70
2006-04-18T21:05:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:04:56+08:00	IMI	6	Web user login, username fs, ip address 220:170.50.44
2006-04-18T21:04:56+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.70
2006-04-18T21:01:20+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:00:50+08:00	IMI	4	Too many users.

Figure 6 Refresh log information operation

Time	Module	Level	Content
2006-04-18T21:26:21+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:19:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:13:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:11:28+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.70
2006-04-18T21:05:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:04:56+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.44
2006-04-18T21:04:56+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.70
2006-04-18T21:01:20+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:00:50+08:00	IMI	4	Too many users.
2006-04-18T21:00:49+08:00	IMI	6	Web user login, username fs, ip address 42.48.181.170

Figure 7 Latest log information list

21.3 Clear Log Information

-

_

If you want to clear the logs displayed in the table, you can click "Clear" button, the operation is shown in figure 8, then the cleared log information list will be displayed, as shown in figure 9.

Refresh Clear			
Time	Module	Level	Content
2006-04-18T21:26:21+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:19:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:13:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:11:28+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.70
2006-04-18T21:05:59+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:04:56+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.44
2006-04-18T21:04:56+08:00	IMI	6	Web user login, username fs, ip address 220.170.50.70
2006-04-18T21:01:20+08:00	DHCLIENT	3	Interface vlan1 received No DHCPOFFER
2006-04-18T21:00:50+08:00	IMI	4	Too many users.
2006-04-18T21:00:49+08:00	IMI	6	Web user login, username fs, ip address 42.48.181.170

Figure 8 Clear log information operation

Refresh Clear				
Time	Module	Level	Content	
Total 0 records.				10 👻 🌩

Figure 9 New log information list

22. SNMP Configuration

If you want to configure SNMP under the web page, you should click "Maintenance" in the top control bar. Then click "SNMP" in the navigation bar, the SNMP page appears, as shown in figure 1.

22.1 SNMP Basic Configuration

F FS 5800-8TF12S		Monitor	Configuration	Maintenance	Network	Save admin Logout
 ⑦ Reboot/Save ③ System Configuration 	Basic Configuration * SNMP Status	🔿 Enable 🛛 💿 Disab	ile (Default: Disable))	1		
Load Configuration File Management	* SNMP Version	All		*		
E Log Management	Community Configuration	Please enter commun	iity name			
SNMP Trap Worm Intercept		(Starts with a letter, o	can only contain (0-9a-zA-Z], character length is [1-256])		
DDoS Intercept ARP Intercept	* Access mode	Add		Ţ		
Currently Sessions Output Description	Community Name	Access	Mode			Delete

Figure 1 SNMP configuration page

Parameter usage

ltem	Description			
SNMP Status	This parameter indicates the SNMP status. It is enabled or disabled			
SNMP Version	This parameter indicates the enabled SNMP versions. All of them enable or enable Version 1, Version 2, and Version 3			
Group Name	SNMP Group name			
Access Mode	Group access mode, read-only or read-write			
Delete	Delete the current group			

22.1.1 Enable SNMP

As shown, SNMP is disabled by default. If you want to use SNMP, you must enable SNMP at first. If you want to enable SNMP, you should follow the steps below:

- (1) Click "Enable" selection box.
- (2) Select the corresponding SNMP version from the drop-down box.
- (3) Click "Apply" button. The operation steps are shown in figure 2.

Basic Configuration		
* SNMP Status	1 • Enable (Default: Disable))	
* SNMP Version	2 All	•
	3 Apply	

Figure 2 SNMP configuration step

22.2 SNMP Group Configuration

SNMPv1 SNMPv2 uses group name authentication. A group is a basic security mechanism. It is used to implement authentication when an SNMP network administrator accesses the SNMP management agent. SNMP packets with different group names will be discarded. The SNMP group is named by a string and becomes the group name. Different groups can have read-only or read-write access modes. Groups with read-only permissions can only query device information, and groups with read-write permissions can also configure devices.

22.2.1 Add SNMP Group

If you want to add a SNMP group, you should follow the steps below:

- (1) Enter the group name. The legal name must start with a letter and can only include 0-9, a-z, A-Z, "_", "-", and the length must be between 1 and 256.
- (2) Select the "Access mode" from the drop-down box.
- (3) Click "Add" button.

The operation steps are shown in figure 3, and the corresponding results are shown in figure 4.

Community Configura	ation			egen de verfinerent over ense F	
* Community Name	Please enter community name (Starts with a letter, can only contain [0-9a-zA-Z,].	, character length is [1-256))	* Access Mode	Read-Only	▼ 2
	Add 3				
	Fig	gure 3 Add SN	IMP commu	unity step	

Community Name	Access Mode	Delete
fs	read-only	Delete

Figure 4 Add SNMP community result

22.2.2 Delete SNMP Group

If you want to delete an existing group, click the "Delete" behind the group list.

Community Name	Access Mode	Delete
fs	read-only	Delete

Figure 5 Delete SNMP community

23. SNMP Trap Configuration

TRAP is a mechanism that provides asynchronous reporting from the agent process to the management station. In order to enable the management station to monitor the managed equipment in a timely and effective manner without excessively increasing the communication load on the network, a trap-guided polling process must be used. The agent process is responsible for reporting an abnormal event to the management station when necessary. After receiving the report of the abnormal event, the management station can inquiry the relevant agent in order to obtain more specific information and further analyze the cause of the event. If you want to configure SNMP trap under the web page, you should click "Maintenance" in the top control bar. Then click "SNMP Trap" in the navigation bar, the SNMP Trap page appears.

23.1 SNMP Trap Basic Configuration

Basic Configuration	
SNMP Trap Enable	Coldstart Trap
	🗌 Linkup Trap
	System Trap
	🗌 Warmstart Trap
	🗌 Linkdown Trap
	Loopback-detect Trap
	Apply

Figure 1 SNMP trap basic configuration page

Parameter usage

ltem	Description
Coldstart Trap	A Coldstart trap signifies that the sending protocol entity is re-initializing itself such that the agent's configuration or the protocol entity implementation may be altered
Linkup Trap	A Linkup trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up
System Trap	A System trap signifies that the protocol has detected a system failure
Warmstart Trap	A Warmstart trap signifies that the sending protocol entity is re-initializing itself such that neither the agent configuration nor the protocol entity implementation is altered
Linkdown Trap	A Linkdown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration
Loopback-detect Trap	A Loopback-detect traps indicate that the protocol has identified loops in the link

23.1.1 Enable SNMP Trap

If you want to enable related SNMP notification types, you should follow the steps below:

(1) Select the notification type you want to enable, and click the checkbox in front of the corresponding type name.

(2) Click the "Apply" button.

The operation is shown in figure 2.





23.2 Trap Server Configuration

Trap Server Configuration	on		
Target Address	Please enter Trap Target Address	Community Name	Please enter Community Name
	(IPv4 or IPv6 Address)		(Start with a letter, can only contain[0-9a-zA-Z,], character length is [1-256))
UDP Port	Please enter UDP Port	Management Interface	
	(0~65535, Default 162)		
	Create		

Figure 3 SNMP trap server configuration page

• Parameter usage

ltem	Description				
Target Address	Destination server address, IPv4 format or IPv6 format				
Community Name	SNMP community name				
UDP Port	Target server corresponding UDP port number				
Management Interface	Whether to forward from the management port				

23.2.1 Create Target SNMP Trap Server

If you want to create a target SNMP trap server, you should follow the steps below:

- (1) Enter server address. The address must be in IPv4 or IPv6 format.
- (2) Enter the name of the community. The legal name must start with a letter and can only include 0-9, a-z, A-Z, "_", "-", and the length must be between 1 and 256.
- (3) Enter the UDP port number corresponding to the server.
- (4) Select whether to forward through the management port. If not, ignore this step.
- (5) Click "Create" button to create SNMP trap server.

The operation steps are shown in figure 4, and the corresponding results are shown in figure 5.

Trap Server Configura	tion	t marmana na sati na mantandina ani nartantana ina sari . T		
Target Address	1	2.2.2.2	Community Name	2 fs
		(IPv4 or IPv6 Address)		(Start with a letter, can only contain[0-9a-zA-Z], character length is [1-256))
UDP Port	3	162	Management Interface	4
		(0~65535, Default 162)		_
	5	Create		

Figure 4 SNMP trap server configuration steps

Refresh				
Target Address	UDP Port	Mgmt-If	Community Name	Delete
2.2.2.2	162	Y	fs	Delete

Figure 5 SNMP trap server configuration result

23.2.2 Delete SNMP Trap Server

If you want to delete an existing target server, click the "Delete" behind the server list.

Refresh				
Target Address	UDP Port	Mgmt-If	Community Name	Delete
2.2.2.2	162	Y	fs	Delete

Figure 6 Delete SNMP trap server

24. Worm Intercept

If you click "Maintenance > Worm Intercept" in the top control bar, the worm intercept list page appears, as shown in figure 1.

FS 55800-8TF125		Monitor Configuration	Maintenance	Network		ave admin Logo
 ⑦ Reboot/Save ※ System Configuration 	Worm Intercept	te Clear Statistics Refre	1 sh			
E Load Configuration	Name	Protocol	Dest-Port	Statistics	Status	Operation
🖹 File Management	NachiBlasterD	tcp	707	0	disable	Edit
Log Management	SQLSlammer	tcp	1433	0	disable	Edit
E SNMP	SQLSlammer	udp	1433	0	disable	Edit
SNMP Trap	SQLSlammer	tcp	1434	0	disable	Edit
🕸 Worm Intercept	SQLSlammer	udp	1434	0	disable	Edit

Figure 1 Worm Intercept configuration list

This chapter describes worm intercept function and viewing worm attack protection information of the switch.

24.1 Worm intercept Configuration

The worm intercept page can view worm attack protection information and add/delete rules to prevent worm attack.

24.1.1 Current Worm Intercept Information

The worm intercept information page appears, as shown in figure 2.

Worm Intercept					
New Delete	Clear Statistics Refresh	n			
Name	Protocol	Dest-Port	Statistics	Status	Operation
NachiBlasterD	tcp	707	0	disable	Edit
SQLSlammer	tcp	1433	0	disable	Edit
SQLSlammer	udp	1433	0	disable	Edit
SQLSlammer	tcp	1434	0	disable	Edit
SQLSlammer	udp	1434	0	disable	Edit
Sasser	tcp	5554	0	disable	Edit
Sasser	tcp	9996	0	disable	Edit

Total: 7records.

Figure 2 Worm intercept information

Parameter usage

ltem	Description
Name	Display worm attack protection rule name
Protocol	Protect this type of protocol message
Dest-Port	Display destination port of worm attack message
Statisitics	Display statistical value of defense attack message
Status	Whether the protection rule is enabled

24.1.2 Add Worm Intercept Rule

If you click "New" button, you can add a worm attack protection rule, the operation is shown in figure 3. And then the worm attack protection configuration page appears, as shown in figure 4.

Worm Intercept					
New Delete	Clear Statistics Refresh				
Name	Protocol	Dest-Port	Statistics	Status	Operation
□ NachiBlasterD	tcp	707	0	disable	Edit
SQLSlammer	tcp	1433	0	disable	Edit
SQLSlammer	udp	1433	0	disable	Edit
SQLSlammer	tcp	1434	0	disable	Edit
SQLSlammer	udp	1434	0	disable	Edit
Sasser	tcp	5554	0	disable	Edit
Sasser	tcp	9996	0	disable	Edit

Total: 7records

Figure 3 Add worm intercept rule operation

Rule Configuration

* Name		(Start with a letter, can only contain[0-9a-zA-Z], character length is 1-20)
* Protocol	▼	
* Destination Port	Please enter	(1-65535)
Enable		
	Apply Back	

Figure 4 Add worm intercept rule configuration

· Parameter usage

ltem	Description
Name	Set worm attack protection name
Protocol	Set Protect protocol type, udp or tcp
Destination Port	Create destination port number of filter message
Enable	Whether to enable this protection rule

- If you want to add the worm attack protection rule, you can follow the following steps: (1) Enter a worm attack protection name in the "Name" textbox, what needs to be noted is the name need to start with a letter, it can only contain [0-9a-zA-Z.-\], character length is 1-20.
- Select protocol type in the "Protocol" dropdown box. (2)
- (3) Enter destination port in the "Destination Port" textbox.
- (4)
- Select enable in the "Enable" square box. Click the "Apply" button to add the new worm attack protection rule. (5)

The operation is shown in figure 5, worm intercept rule will be added to the end of the table is shown in figure 6 and you can also see the total rule numbers at the end of the table. If there are too many rules, you can drag the mouse to pull down the page.

Rule Configuration			
* Name	1	feisu	(Start with a letter, can only contain[0-9a-zA-Z], character length is 1-20)
* Protocol	2	▼ ▼	
* Destination Port	3	123	(1-65535)
Enable			
	4	Apply Back	

Figure 5 Add worm intercept rule configuration

New Delete	Clear Statistics Refr	esh			
Name	Protocol	Dest-Port	Statistics	Status	Operation
□ NachiBlasterD	tcp	707	0	disable	Edit
SQLSlammer	tcp	1433	0	disable	Edit
SQLSlammer	udp	1433	0	disable	Edit
SQLSlammer	tcp	1434	0	disable	Edit
SQLSlammer	udp	1434	0	disable	Edit
Sasser	tcp	5554	0	disable	Edit
Sasser	tcp	9996	0	disable	Edit
🗇 feisu	tcp	123	0	disable	Edit

Total: 8records.

Figure 6 New worm intercept rule information

24.1.3 Delete Worm Intercept Information

If you want to delete the specified worm intercept information, you can follow the following steps:

- (1) Select this specified worm attack protection information which you want to delete.
- (2) Click "Delete" button.
- (3) Confirm to delete the selected worm attack protection information and page appears as shown in figure 7, if you click "Confirm" button, you can delete this worm intercept rule, if you click "cancel" button, you can cancel the operation. The operation is shown in figure 7.



Figure 7 Delete worm intercept information

24.1.4 Clear the Defense Attack Packet Statistics

If you want to clear the specified worm attack protection packet statistics, you can follow the following steps:

- (1) Select this specified worm attack protection information which you want to clear statistics.
- (2) Click "Clear Statistic" button.
- (3) Confirm to clear statistics of the selected worm attack protection information and page appears as shown in figure 8, if you click "Confirm" button, you can delete this worm intercept rule, if you click "cancel" button, you can cancel the operation. The operation is shown in figure 8.

Worm Intercept					
New Delete	Clear Statistics Ref	resh			
Name	Protocol	Dest-Port	Statistics	Status	Operation
NachiBlasterD	tcp	707	0	disable	Edit
SQLSlammer	tcp	ps	×	disable	Edit
SQLSlammer	udp			disable	Edit
SQLSlammer	tcp			disable	Edit
SQLSlammer	udp	I Are you sure to Cle	ear Statistics?	disable	Edit
Sasser	tcp			disable	Edit
Sasser	tcp	3 Confirm	Cancel	disable	Edit
1 🗹 feisu	tcp	123	0	disable	Edit

Total: 8records.

Figure 8 Clear statistics operation

24.1.5 Refresh Worm Intercept Page

If you add/delete worm intercept information or clear statistics but the operation doesn't Immediately effect, please click "Refresh" button to refresh the worm intercept page and the operation is shown in figure 9.

Worm Intercept					
New	Delete Clear Statistics Refr	esh			
Name	Protocol	Dest-Port	Statistics	Status	Operation
□ NachiBlasterD	tcp	707	0	disable	Edit
SQLSlammer	tcp	1433	0	disable	Edit
SQLSlammer	udp	1433	0	disable	Edit
SQLSlammer	tcp	1434	0	disable	Edit
SQLSlammer	udp	1434	0	disable	Edit
□ Sasser	tcp	5554	0	disable	Edit
Sasser	tcp	9996	0	disable	Edit
🗌 feisu	tcp	123	0	disable	Edit

Total: 8records.

Figure 9 Refresh worm intercept page

25. DDoS Intercept

A DDoS (distributed denial of service attack) refers to multiple attackers in different locations launching attacks on one or several targets simultaneously, or an attacker controls multiple machines in different locations, and use these machines to attack the victims at the same time. Because the attack points are distributed in different places, this type of attack is called a distributed denial of service attack. In order to prevent DDoS attacks, you can set DDoS interception. DDoS interception settings can limit DDoS attacks according to different types of attacks.

If you want to configure DDoS interception under the web page, you should click "Maintenance" in the top control bar. Then click "DDoS Intercept" in the navigation bar, the DDoS Intercept page appears.

25.1 DDoS Intercept Page

FS 55800-8TF125		Monitor	Configuration	* Maintenance	Network	Save admin Logou
				1		
() Reboot/Save	DDoS Intercept Settings					
System Configuration	Parameter Information	ICMP Flood Intercept	Please enter		/ pps (0-1000)	
E Load Configuration						
File Management		UDP Flood Intercept			/ pps (0-1000)	
Log Management		SYN Flood Intercept	Please enter		/ pps (0-1000)	
E SNMP		Small-packet Attack Intercept			bytes (28-65535)	
SNMP Trap		Course Attack Intercent				
🖄 Worm Intercept		Frage Attack Intercept				
DDoS Intercept 2		MAC Equal Intercept				
ARP Intercept		IP Equal Intercept				
Currently Sessions		Apply				
R User Management						
			Copyrig	ht © 2009-2020 FS.COM Inc	. All Rights Reserved.	

Figure 1 DDoS intercept page

• Parameter usage

i alameter abage	
ltem	Description
ICMP Flood Intercept	ICMP FLOOD attack sends a large number of ping packets to the destination host , consuming host resources. This interception is used to defend against ICMP attacks
UDP Flood Intercept	The UDP Flood attack is to forge a large number of UDP packets to impact the server, resulting in service failure
SYN Flood Intercept	The SYN Flood attack is a vulnerability that uses the TCP three-factor authentication mechanism to send a large number of fake SYN packets, causing the server to crash
Small-packet Attack Intercept	Small-packet Attack includes UDP and SYN attack,etc. Because most Small-packets are meaningless and are often used for DDoS attacks, they can be intercepted based on Small-packets
Smurf Attack Intercept	The Smurf attack is a virus attack named after the program "Smurf" that originally launched the attack. This attack method uses a combination of IP spoofing and ICMP reply methods to flood the target system with a large number of network transmissions, causing the target system to refuse to serve normal systems

Item	Description		
Fraggle Attack Intercept	Fraggle attack is similar to Smurf attack, but it uses UDP reply message instead of ICMP reply		
MAC Equal Intercept	The MAC Equal attack is to mimic ARP request packets with both the source and destination MACs as the destination host's MAC, causing the host to constantly consume its own memory and crash		
IP Equal Intercept	IP Equal attack is to imitate ICMP Ping packets whose source IP and destination IP are the destination host IP, causing the host to constantly consume its own memory and cause a crash.		

The interception of ICMP flood, SYN flood, UDP flood and Small-packet attack is based on setting the PPS (packet per second) threshold to achieve defense functions. Therefore, before using this interception, you need to set a threshold. The threshold range is behind the corresponding textbox.

25.2 DDoS Intercept Setting

If you want to enable one or more of the above interception methods, you should follow the steps below.

- (1) Select the interception methods you want to enable, and click the checkbox in front of the corresponding methods name.
- (2) If the method is ICMP flood, SYN flood, UDP flood, or Small-packet Attack, you should set the corresponding threshold, and fill in the threshold you want to set in the text edit box after the method name (Note: The range of the threshold is in parentheses after the textbox). If it is not the above four methods, ignore this step.
- (3) Click the "Apply" button.
- The operation steps are shown in figure 2.

DDoS Intercept Settings					
Parameter Information		CICMP Flood Intercept	Please enter	/ pps	(0-1000)
		UDP Flood Intercept	Please enter	/ pps	(0-1000)
	1	2	Please enter	/ pps	(0-1000)
		Small-packet Attack Intercept	Please enter	bytes	(28-65535)
		Smurf Attack Intercept			
		Fraggle Attack Intercept			
		IP Equal Intercept			
	3	Apply			

Figure 2 DDoS intercept setting

26. ARP Intercept

If you click "Maintenance ->ARP Intercept" the ARP Intercept configuration list page appears, as shown in figure 1. If you want to enable and set arp intercept you should follow the steps below:

- (1) Select "Arp Intercept" in this page.
- (2) Set the threshold of the arp intercept.(3) Click "Apply" button.

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network	Save admin Logout
() Reboot/Save	Arp Intercept Settings					
System Configuration	Parameter Information	Arp Intercept	2560		/ pps	
E Load Configuration			2 (0-1000000;if the val	lue is set to 0, no dynamic /	ARP entry will be learnt again.)	
📄 File Management		3 Apply				
Log Management						
I SNMP						
SNMP Trap						
(1) Worm Intercept						
ODoS Intercept						
ARP Intercept						
Currently Sessions						
R User Management						
		Figure	1 ARP interce	ept configura	tion list	

• Parameter usage

ltem	Description
PPS	Packets per second

NOTE: When you enable Arp Intercept and set threshold of PPS, every IP that exceeds the threshold will be blocked.

27. Currently Sessions

If you click "Maintenance -> Currently Sessions" in the top control bar, the currently session list page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	Configuration	X Maintenance	Network	Save admin Logout
	Currently Web Sessions			1		
C Reboot/Save	Delan Refuel					
System Configuration	Deteter Neiresi					
E Load Configuration	User Name		Session ID		Expire Time	Client IP
🖹 File Management	admin		1592623855		2020-06-20 11:30:58	192.168.1.6
Log Management	🔲 admin		1592620382		2020-06-20 11:36:15	192.168.1.25 (*)
I SNMP	🗆 admin		1592619776		2020-06-20 11:25:52	192.168.1.21
SNMP Trap						
🖄 Worm Intercept						
ODoS Intercept						
ARP Intercept						
Currently Sessions 2						
옷 User Management						

Figure 1 Current sessions list

This chapter describes the users and sessions configuration function of the device. Currently sessions display current web sessions information, and you can delete some sessions.

27.1 Current Sessions Information

Currently sessions display current web sessions information, as shown in figure 2, or you can click "Currently Sessions -> Refresh" button in the title bar, current sessions page will be refreshed and , the operation is shown in figure 3.

Currently Web Sessions Delete Refresh			
User Name	Session ID	Expire Time	Client IP
🗋 admin	1592623855	2020-06-20 11:30:58	192.168.1.6
🗋 admin	1592620382	2020-06-20 11:44:42	192.168.1.25 (*)

Figure 2 Current sessions information

Currently Web Sessions Delete Refresh			
User Name	Session ID	Expire Time	Client IP
🗋 admin	1592623855	2020-06-20 11:30:58	192.168.1.6
🗋 admin	1592620382	2020-06-20 11:44:42	192.168.1.25 (*)

Figure 3 Refresh current sessions information
• Parameter usage

Item	Description
User Name	Display user name
Session ID	Display session id
Expire Time	Display the expire time
Client IP	Display client IP address

27.2 Delete Current Sessions

If you want to delete some sessions, you can follow the following steps:

- Choose one or more the sessions which you want to delete. (1)
- (2) Click "Delete" button.
- (2) Click Delete Button.
 (3) It will appear tips page to note you to confirm the operation, if you click "Delete" button, it will delete the session; if you click "Cancel" button, you will cancel the delete operation.
 The operation is shown in figure 4, the result page is shown in figure 5.

Currently Web Sessions			
2 Delete Refresh			
User Name	Session ID	Expire Time	Client IP
1 🗹 admin	1592623855	2020-06-20 11:30:58	192.168.1.6
🗋 admin	1592620: tips	× ^{1:42}	192.168.1.25 (*)
	Are you sure to	o delete the selected session ?	
	3 Confirm	Cancel	
	Figure 4 Delete ses	sions operation	

Currently Web Sessions			
Delete Refresh			
User Name	Session ID	Expire Time	Client IP
🗌 admin	1592620382	2020-06-20 11:47:58	192.168.1.25 (*)

Figure 5 New current sessions information

28. User Management

If you click "Maintenance ->User Management" in the top control bar, the User Management configuration list page appears as shown in figure 1.

FS SSB00-BTF12S		Monitor	Configuration	Maintenance	Network	Save admin Logo
 ⑦ Reboot/Save System Configuration 	User management Add Delete Refresh			1		
E Load Configuration	User Name		Privilege		Password	Operation
File Management	🗋 admin		4		*	Edit
Log Management						
I SNMP						
SNMP Trap						
🖄 Worm Intercept						
Ø DDoS Intercept						
ARP Intercept						
Currently Sessions						
Q User Management 2						

Figure 1 User management configuration list

This chapter describes user management configuration function.

28.1 Add User

If you click " Add" in User Management page you will see figure 2 and figure 3 .

FS [55800-8TF125]		Monitor	Configuration	Maintenance	A Network	Save admin Logout
 ⑦ Reboot/Save © System Configuration 	User management Add Delete Refresh					
E Load Configuration	User Name		Privilege		Password	Operation
📄 File Management	🔲 admin		4			Edit
Log Management						
I SNMP						
SNMP Trap						
③ Worm Intercept						
ODoS Intercept						
ARP Intercept						
Currently Sessions						
A User Management						

Figure 2 User add page

FS 55800-8TF125		Monitor	Configuration	Maintenance	Network	Save admin Logout
(5 Bahaat/Faus	Add/Modify User					
System Configuration	User Name	Please enter		(Start with	a letter,can only contain[0-9a-zA-Z].c	character length is (1,32))
E Load Configuration	Password	Please enter				
🖹 File Management	Confirm Pareword	Diagra antor				
Log Management	Commin Password					
SNMP	Privilege	4		(1-4)		
SNMP Trap		Apply Back				
③ Worm Intercept						
Ø DDoS Intercept						
ARP Intercept						
Currently Sessions						
A User Management						

Figure 3 Add/Modify User page

· Parameter usage

Item	Description
User name	user name
Password	user`s password
Confirm password	input Pssword again
Privilege	Privilege of User(1-4)

NOTE:

- (1) User Privilege Level 1: You can execute commands for functions such as network diagnostics. Including commands such as ping, tracert, and telnet. The results of executing commands at this level cannot be saved to the configuration file.
- (2) User Privilege Level 2: It can execute commands for system maintenance, business fault diagnosis, and other functions. Including commands such as debugging and terminal. The results of executing commands at this level cannot be saved to the configuration file.
- (3) User Privilege Level 3: It can execute commands for service configuration, including network-level commands such as routing, to provide network services to users.
- (4) User Privilege Level 4: At the highest level, you can run all commands: commands related to the basic operation of the system and functions of the system support module. These commands provide support to the business. Including file system, FTP, TFTP, XModem download, user management commands, level setting commands, etc.

28.2 Edit User

If you click "Edit" after you selected a user in User Management page you will see figure 4 and figure 5.

User management			
Add Delete Refresh			
User Name	Privilege	Password	Operation
🗋 admin	14	*	Edit
□ admin_guest	4	*	Edit

Figure 4 Edit user

Add/Modify User		
User Name	admin_guest	(Start with a letter,can only contain[0-9a-zA-Z,],character length is [1,32])
Password	Please enter	
Confirm Password	Please enter	
Privilege	4	(1-4)
	Apply Back	

Figure 5 Edit user

The corresponding operation steps are the same as those of User Add.

28.3 Delete User

If you click delete after you selected a user in User Management page you will see figure 6. If you want to delete user, you can follow the following steps:

- (1) Select the user by selecting the check box in front of the user name.
- (2) Click "Delete" button.

User management			
Add 2 Delete Refresh			
User Name	Privilege	Password	Operation
🗋 admin	4	*	Edit
1 🔽 admin_guest	4 tips	×	Edit
	() Are you sure to de	ilete selected users?	
	3 Confirm	Cancel	

Figure 6 Delete user

28.4 Refresh

User management			
Add Delete Refresh			
User Name	Privilege	Password	Operation
🗋 admin	4	*	Edit
🗋 admin_guest	4	×	Edit

Figure 7 Refresh

NOTE: The refresh button is to refresh the current page.

29. IP Routing

If you click "Network ->IP Routing" in the top control bar, the IP routing configuration list page appears, as shown in figure 1.

FS SSB00-BTF12S		Monitor Config	taintenance	1 Network	Save admin Logout
IP Routing 2 Ping Traceroute	IPv4 Routing Table Information IPv4 Routing Table Information Protocol All	IPv4 Static Route Information	• Query		
	Destination	Mask	Protocol	Nexthop	Outgoing Interface
	192.168.1.0	255.255.255.0(24)	Direct		vlan1
	192.168.1.126	255.255.255.255(32)	Direct		vlan1
	Total 2 records.				10 💌 👄

Figure 1 IP routing configuration list

This chapter describes IP static route configuration function and viewing routing information of the device.

29.1 IPv4 Route

By choosing different routing protocols, you can view the protocol routing information you want to know.

29.1.1 Current Routing Information

If you click "IP Routing -> IPv4 Routing table information" in the title bar, the IPv4 routing table information page appears, as shown in figure 2.

1 Pip Routing Ping	2 IPv4 Routing table IPv4 Routing table	IPv4 Static Route Information					
V Iraceroute	Protocol	All	Quer				
	Destination	Mask	Protocol	Nexthop	C	Dutgoing Int	erface
	1.1.1.235	255.255.255.255(32)	Direct		ł	oopback0	
	Total 1 records.				10	•	+

Figure 2 IPv4 routing table information

Parameter usage

Item	Description
Destination	Display destination IP address of the route
Mask	Display IP address mask of the Destination
Protocol	Display the kind of route
Nexthop	Display nexthop of the route
Outgoing Interface	Display outgoing interface of the route

If you want to view routing information for a protocol, please select the routing protocol from the "Protocol" dropdown box, and then click the "Query" button, the operation is shown in figure 3.

IPv4 Routing tab	IPv4 Static Route	e Information	
v4 Routing ta	ble information 1	2	
Protocol	All	Query	
Destination	Aii BGP Direct	Nexthop	Outgoing Interfac
1.1.1.235	OSPF RIP Static		loopback0



29.2 IPv4 Static

Through the IPv4 static route configuration function, you can add/modified/delete the static route on device.

29.2.1 IPv4 Static Route Information

If you click "IP Routing -> IPv4 Static Route information" in the title bar, the IPv4 static routing information page appears, as shown in figure 4.

● IP Routing 1○ Ping	IPv4 Routing table information	IPv4 Static Route Information	2		
😰 Traceroute	New Delete				
	Destination	Mask	Nexthop	Distance	Operate
	2.2.2.0	255.255.255.0	1.1.1.1	1	Edit
	3.3.3.0	255.255.255.0	1.1.1.1	10	Edit
	Total 2 records.				10 💌 🗭

Figure 4 IPv4 static routing information

• Parameter usage

ltem	Description
Destination	Display destination IP address of the route
Mask	Display IP address mask of the Destination
Nexthop	Display nexthop of the route
Distance	Display routing distance value
Operate	Display that static routing table entries can be edited

29.2.2 Add IPv4 Static Route

If you click "New" button, you can add a static route, the operation is shown in figure 5, and then the IPv4 static routing configuration page appears, as shown in figure 6.

IPv4 Routing table information	IPv4 Static Route Information	
IPv4 Static Route Information —		
New Delete		
	Figure 5 Add IPv4 static route operation	

IP Routing	IPv4 Routing Table Infor	mation	IPv4 Static Rou	ute Information		
Ping	IPv4 Static Route Item					
😰 Traceroute	• Destination					
	* Mask	255.255.255.0(2	4)		÷	
	Nexthop					
	* Distance	1				(1-255, default 1)
		Apply	Back			

Figure 6 Add IPv4 static route

Parameter usage

ltem	Description
Destination	Set specify destination IP address
Mask	Set specify IP address mask for destination
Nexthop	Set specify nexthop IP address
Distance	Set specify the distance of the static route(default is 1)

If you want to add the specified static route, you can follow the following steps:

- (1) Enter an IP address in the "Destination" textbox, such as the IP address of other network device.
- (2) Select the destination address mask in the "mask" dropdown box.
- (3) Enter nexthop IP address in the "Nexthop" textbox.
- (4) Enter route distance in the "Distance" textbox.
- (5) Click the "Apply" button.

The operation is shown in figure 7, routing successfully configured table item information is shown in figure 8.

IPv4 Routing table in	nformation IPv4 Static Route Information		
IPv4 Static Route It	tem		
* Destination	3.3.3.3	(0.0.0.0) 1	
* Mask	255.255.255.0(24)	• 2	
* Nexthop	1 , 1 , 1 , 1	(0.0.0.0) 3	
* Distance	10	(1-255, default 1) 4	
5	Apply Back		

Figure 7 Add IPv4 static route configuration

Pv4 Routing table information	IPv4 Static Route Information			
4 Static Route Information				
New Delete				
New Delete				
New Delete	Mask	Nexthop	Distance	Operate
New Delete Destination 2.2.2.0	Mask 255.255.255.0	Nexthop 1.1.1.1	Distance 1	Operate Edit

Figure 8 New IPv4 static route information

29.2.3 Delete IPv4 Static Route

- If you want to delete the specified static route, you can follow the following steps:
- (1) Select this specified static route which you want to delete.
- (2) Click "Delete" button.
- (3) It will appear tips page to note you to confirm the operation, as shown in figure 9, if you click "Delete" button, it will delete the static route; if you click "Cancel" button, you will cancel the delete operation.

IPv4 Routing Table Information	IPv4 Static Route Information					
IPv4 Static Route Information						
 Destination 	Mask			Distance		Operation
2.2.2.0	255.255.255.0	Tips	~	1		Edit
1 3.3.3.0	255.255.255.0			10		Edit
Total 2 records		Are you sure to delete the selected IP addre	ess?		10	
					10 4	4
		3 Confirm Cancel				

Figure 9 Delete IPv4 static route

29.2.4 Modify IPv4 Static Route

If you want to modify the configuration to specify static routing, please click "Edit" button, the operation is shown in figure 10, modifies the specified static routing page to appear, as shown in figure 11.

IPv4 Routing table information	IPv4 Static Route Information			
IPv4 Static Route Information				
Destination	Mask	Nexthop	Distance	Operate
2.2.2.0	255.255.255.0	1.1.1.1	1	Edit

Figure 10 Modify IPv4 static route operation

FS 55800-8TF125			Monitor	Configuration	X Maintenance	Network	Save) admin	Logout
IP Routing	IPv4 Routing Table Info	rmation	IPv4 Static Route In	formation					
Ping	IPv4 Static Route Iten	n							
Traceroute	Destination	2 . 1	2 . 2	. 0					
	• Mask		24)		*				
	Nexthop	1	1 . 1	1.1					
	Distance	1			(1~255, default 1)				
		Apply	Back						

Figure 11 Modify IPv4 static route

• Parameter usage

ltem	Description
Destination	Display specify destination IP address
Mask	Display specify IP address mask for destination
Nexthop	Set specify nexthop IP address



Distance

Set specify the distance of the static route(default is 1)

If you want to modify the nexthop and distance of the static route, you can follow the following steps:

- (1)
- Modify nexthop IP address in the "Nexthop" textbox. Select the destination address mask in the "mask " dropdown box. (2)
- Modify route distance in the "Distance" textbox. Click the "Apply" button. (3)
- (4)

The operation is shown in figure 12.

IPv4 Routing table information		IPv4 Static Rout	e Information	
IPv4 Static Route It	em			
* Destination	2.	2.2	. 0	
* Mask	255.255.255.	0(24)		×
* Nexthop	1 ,	1.1	. 10	(0.0.0.0) 1
* Distance	22			(1-255, default 3) 2
3	Apply	Back		

Figure 12 Modify IPv4 static route configuration

30. Ping

Users can take advantage of these features to diagnose and detect network and analyze error information. If you click "Network-> Ping" in the top control bar, the Ping page appears, as shown in figure 1.

FS 55800-8TF125			Monitor	Configuration	X Maintenance	I Network	Save admin	Logout
IP Routing	Ping Settings							
Ping 2	VRF ID	mgmt vrf			*			
Traceroute	Destination IP	10 . 10	. 25 .	30				
		Ping						
				Copyrigh	t © 2009-2020 FS.COM Inc	. All Rights Reserved.		

Figure 1 Ping settings

• Parameter usage

ltem	Description
VRF ID	Specify ping port. Mgmt VRF means management port and default VRF means VRF1
Destination IP	Destination IP

If you want to implement ping test, you can perform the following steps:

- (1) Choose the VRF ID.
- (2) Enter target IP address is to be tested in Destination IP.
- (3) Click the "Ping " button to test the connection.

The operation is shown in figure 2, implement ping test result is shown in figure 3.

VRF ID	mgmt vrf		• 1	
Destination IP	10 . 10 . 25	. 30	(0.0.0.0) 2	
	Ping 3			

ID	mgmt vrf	•	
ination IP	10 . 10 . 25 . 30	(192.168.1.1)	
	Ping		
	Ping		
	Ping PING 10.10.25.30 (10.10.25.30) from 10.32.133.252 MAN From 10.32.133.252 iomp_seq=1 Destination Host Unread	VRF: 56(84) bytes of data. able	
	Ping PING 10.10.25.30 (10.10.25.30) from 10.32.133.252 MAN From 10.32.133.252 icmp_seq=1 Destination Host Unread From 10.32.133.252 icmp_seq=2 Destination Host Unread From 10.32.133.252 icmp seq=3 Destination Host Unread	VRF: 56(84) bytes of data. able able able	
	Ping PING 10. 10. 25. 30 (10. 10. 25. 30) from 10. 32, 133. 252 MAN From 10. 32, 133. 252 iomp_seq=1 Destination Host Unread From 10. 32. 133. 252 iomp_seq=2 Destination Host Unread From 10. 32. 133. 252 iomp_seq=3 Destination Host Unread From 10. 32. 133. 252 iomp_seq=4 Destination Host Unread From 10. 32. 133. 252 iomp_seq=4 Destination Host Unread	VRF: 56(84) bytes of data. able able able able	
	Ping PING 10. 10. 25. 30 (10. 10. 25. 30) from 10. 32, 133. 252 MAN From 10. 32, 133. 252 icmp_seq=1 Destination Host Unread From 10. 32, 133. 252 icmp_seq=2 Destination Host Unread From 10. 32, 133. 252 icmp_seq=4 Destination Host Unread From 10. 32, 133. 252 icmp_seq=6 Destination Host Unread	VRF: 56(84) bytes of data. able able able able able	
	Ping PING 10. 10. 25. 30 (10. 10. 25. 30) from 10. 32. 133. 252 MAM From 10. 32. 133. 252 iomp_seq=1 Destination Host Unread From 10. 32. 133. 252 iomp_seq=2 Destination Host Unread From 10. 32. 133. 252 iomp_seq=4 Destination Host Unread From 10. 32. 133. 252 iomp_seq=5 Destination Host Unread From 10. 32. 133. 252 iomp_seq=5 Destination Host Unread 	VRF: 56(84) bytes of data. able able able able	

Figure 3 Implement ping test result

31. Traceroute

31.1 Traceroute

Tracert is a utility program used to confirm the route that IP packet will take to access the target. Tracert determines the route from a host to another host in the network by sending ICMP error packets with time-to-live (TTL) values. If you click "Network ->Traceroute" in the top control bar, the trace route settings page appears, as shown in figure 1.

FS 55800-8TF125		Monitor	Configuration	% Maintenance	Network	Save admin	Logout
IP Routing	Trace Route Settings						
ES Pring €? Traceroute 2	Destination IP 10 . 10	. 25 . 30)				
	Traceroute						
			Copyright ©	2009-2020 FS.COM Inc	: All Rights Reserved.		

Figure 1 Trace route settings

• Parameter usage

Item	Description					
VRF ID	Specify ping port. Mgmt VRF means management port and default VRF means VRF1					
Destination IP	Destination IP					

31.2 Implement Tracert Ping Test

Through the IPv4 static route configuration function, you can add/modified/delete the static route on switch.

If you want to implement tracert ping test, you can follow the following steps:

- (1) Choose the VRF ID.
- (2) Enter target IP address is to be tested in Destination IP.

(3) Click Trace Route button to test route from source address to destination address.

(4) The result will display under the configuration panel.

The operation is shown in figure 2, implement tracert ping test result is shown in figure 3.

IP Routing	Trace Route Sett	tings	······································
Ping	VRF ID	1 mgmt vrf	-
😰 Traceroute	Destination IP	2 10 . 10 . 25 . 30	(192.168.1.1)
		3 Traceroute	
			Copyright © 2009-2020 FS.COM Inc . All Rights Reserve



	Trace Route Setti	nas	
IP Routing			
Ding	VRF ID	mgmt vrf 👻	
😰 Traceroute	Destination IP	10 . 10 . 25 . 30	(192.168.1.1)
		Traceroute	
	_		7
	tra 1 2	ceroute to 10.10.25.30 (10.10.25.30), 30 hops max, 38 byte packets * 192.168.1.1 (192.168.1.1) 4021.233 ms H * 192.168.1.1 (192.168.1.1) 4020.848 ms H * 4023.367 ms H	
한 동안은 모두 동안을 받는 것이 같아요.		Copyright © 20	09-2020 FS.COM Inc . All Rights Reserved.

Figure 3 Implement tracert ping test result

32. Virtual Cable Test

If you click "Network->Virtual Cable Test" in the top control bar, the virtual cable test page appears, as shown in figure 1.

FS 55850-24T165	Monitor	Configuration	Maintenance	1 Annetwork	Save	admin	Logout
P Routing Virtua Virt	I Cable Test Settings Notes: VCT at 100Mb pet Interface: eth-0-9 1000BASE_T Test	Configuration	Maintenance	Network			
		Copyright	© 2009-2020 FS.COM Inc . 1	All Rights Reserved.			

Figure 1 Virtual cable test page

This section mainly describes how to use virtual cable test to detect cable condition and error type.

Parameter usage

ltem	Description
Target Interface	Select the target interface to run VCT

If you want to perform virtual cable detection on a certain port, you can select the port you want to detect from the drop-down box, then click the "Detection" button, the operation is shown in figure 2, and the detection result is shown in figure 3.



Figure 2 Virtual cable test operation

Virtual Cable Te	est							
VCT Settings			Notes: VCT at 100Mb/s link will cause port down awhile.					
Target Interfac	eth-0-9 1000BASE_T 100Mb/s					•		
			Test					
			_					
Interface		Speed	Local_pair	Pair_	length R	emote_pair	Pair_status	
e	eth-0-9		Pair A Pair B Pair C Pair D	0 +/- 57 +/- 0 +/-	5 meters 5 meters 8 meters	Present Present Present	Normal Normal Abnormal (open)	

Figure 3 Virtual cable test result



https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.

Copyright © 2009-2022 FS.COM All Rights Reserved.