



## **SW-MNG-24GE4/10GSFP**

**24-Port 10/100/1000Mbps + 4-Port 10Gbps SFP  
Managed Ethernet Switch**



## **User Manual**

**Ver 1.0 | 6/15/2016**

# Table of Contents

<b>Chapter 1 Product Introduction.....</b>	<b>12</b>
1.1 Product Overshow .....	12
1.2 Features .....	12
1.3 Package Contents .....	12
<b>Chapter 2 External Component Description.....</b>	<b>13</b>
2.1 Front Panel .....	13
2.2 Rear Panel.....	14
<b>Chapter 3 Installing and Connecting the Switch .....</b>	<b>15</b>
3.1 Installation.....	15
3.1.1 Desktop Installation.....	15
3.1.2 Rack-mountable Installation in 19-inch Cabinet .....	15
3.1.3 Power on the Switch .....	16
3.2 Connect Computer (NIC) to the Switch.....	16
3.3 How to Login the Switch .....	17
<b>Chapter 4 Switch Configuration.....</b>	<b>19</b>
4.1 Switch basic configuration.....	19
4.1.1 Switch basic configuration. ....	19
4.1.1.1 Login user configuration.....	19
4.1.1.2 Login user authentication method configuration. ....	20
4.1.1.3 Login user security IP management.....	20
4.1.1.4 Basic configuration.....	21
4.1.1.5 Save current running-configuration. ....	21
4.1.2 SNMP configuration. ....	22
4.1.2.1 SNMP authentication.....	22
4.1.2.2 SNMP management. ....	24
4.1.3 SSH management. ....	25
4.1.3.1 Switch on-off SSH.....	25
4.1.3.2 SSH management.....	26
4.1.4 Firmware update.....	26
4.1.4.1 TFTP service.....	26
4.1.4.2 FTP service.....	27
4.1.5 Telnet server configuration.....	28
4.1.5.1 Telnet server state.....	29
4.1.5.2 Max number of telnet access connection.....	29
4.1.6 Maintenance and debugging command.....	29
4.1.6.1 Debug command.....	30
4.1.6.2 Show clock.....	30
4.1.6.3 Show cpu usage.....	30
4.1.6.4 Show cpu show memory usage.....	31
4.1.6.5 Show flash.....	31
4.1.6.6 Show running-config.....	31
4.1.6.7 Show switchport interface.....	31

---

4.1.6.8 Show tcp.....	32
4.1.6.9 Show udp.....	32
4.1.6.10 Show telnet login.....	32
4.1.6.11 Show version. ....	33
4.2 Module management. ....	33
4.2.1 Show boot-files. ....	33
4.2.2 Set Boot IMG and Startup-Config. ....	34
4.3 Port configuration.....	34
4.3.1 Ethernet port configuration.....	34
4.3.1.1 Port layer 1 attribution configuration. ....	35
4.3.1.2 Bandwidth control configuration.....	36
4.3.1.3 Switchport description. ....	37
4.3.1.4 Port combo forced mode config.....	37
4.3.1.5 Port scan mode. ....	38
4.3.2 VLAN interface configuration.....	38
4.3.2.1 Add interface configuration. ....	38
4.3.2.2 L3 interface IP address mode configuration. ....	38
4.3.3 SPAN configuration.....	39
4.3.3.1 SPAN configuration.....	39
4.3.4 Loopback-detection configuration.....	40
4.3.4.1 Port Loopback-detection mode configuration. ....	40
4.3.4.2 VLAN Loopback-detection configuration.....	41
4.3.4.3 Loopback-detection interval-time configuration.....	41
4.3.4.4 Loopback-detection control recovery configuration. ....	41
4.3.5 Isolate-port configuration.....	42
4.3.5.1 Isolate-port configuration. ....	42
4.3.5.2 Interface join group config. ....	42
4.3.5.3 Show Isolate-port group.....	42
4.3.6 Port storm-control config .....	43
4.3.6.1 Storm-control config.....	43
4.3.7 Port rate-violation config.....	43
4.3.7.1 Port rate-violation config .....	44
4.3.8 Port virtual-cable-test config.....	44
4.3.8.1 Virtual-cable-test configuration.....	45
4.3.9 Port debug and maintenance. ....	45
4.3.9.1 Show port information. ....	45
4.3.9.2 Show entire traffic information.....	46
4.3.9.3 Show rate violation port.....	46
4.3.10 ULDP configuration.....	47
4.3.10.1 ULDP enable config.....	47
4.3.10.2 ULDP Hello message config. ....	48
4.3.10.3 ULDP recovery time config.....	48
4.3.10.3 Show ULDP configuration.....	48
4.3.11 LLDP configuration.....	48

---

4.3.11.1 LLDP configuration.....	49
4.3.11.2 LLDP port status config. ....	49
4.3.11.3 LLDP tx-interval config. ....	50
4.3.11.4 LLDP msgTxHold config. ....	50
4.3.11.5 LLDP transmit delay config.....	50
4.3.11.6 LLDP notification interval config.....	50
4.3.11.7 LLDP neighbors max-num config. ....	51
4.3.11.8 LLDP too many neighbors config. ....	51
4.3.11.9 LLDP transmit optional tlv config. ....	51
4.3.11.10 show LLDP configuration.....	52
4.3.12 LED shutoff configuration.....	52
4.3.12.1 Time Range configuration.....	52
4.3.12.2 LED shutoff config.....	53
4.3.13 Jumbo packet forwarding configuration.....	53
4.4 MAC address table configuration. ....	53
4.4.1 MAC address table configuration.....	54
4.4.2 Configuration MAC address.....	54
4.4.3 Delete MAC address.....	54
4.4.4 MAC address query.....	55
4.5 VLAN configuration. ....	55
4.5.1 VLAN configuration. ....	55
4.5.1.1 VLAN ID configuration.....	56
4.5.1.2 Assign ports for VLAN. ....	56
4.5.1.3 Set port mode(access/hybrid/trunk). ....	57
4.5.1.4 VLAN setting for hybrid port. ....	57
4.5.1.5 VLAN setting for trunk port. ....	58
4.5.1.6 Private-vlan association. ....	58
4.5.2 GVRP configuration. ....	58
4.5.2.1 Enable global GVRP. ....	59
4.5.2.2 Enable GVRP on port. ....	59
4.5.2.3 GARP configuration. ....	59
4.5.3 VLAN-translation configuration.....	59
4.5.3.1 Enable/Disable VLAN-translation. ....	60
4.5.3.2 Add/Delete VLAN-translation.....	60
4.5.3.3 VLAN-translation miss drop configuration.....	61
4.5.3.4 Show VLAN-translation. ....	61
4.5.4 Dynamic VLAN configuration.....	61
4.5.5 Dot1q tunnel configuration.....	62
4.5.5.1 Enable dot1q tunnel.....	62
4.5.5.2 Dot1q tunnel tpid configuration. ....	62
4.6 IGMP snooping configuration.....	63
4.6.1 Switch on-off IGMP snooping. ....	63
4.6.2 IGMP snooping port enable. ....	63
4.6.3 IGMP snooping configuration. ....	64

---

4.6.4 IGMP snooping mrouter port configuration. ....	64
4.6.5 IGMP snooping query configuration. ....	65
4.7 MLD snooping configuration. ....	65
4.7.1 Switch on-off MLD snooping. ....	65
4.7.2 MLD snooping port enable. ....	66
4.7.3 MLD snooping configuration. ....	66
4.7.4 MLD snooping mrouter port configuration. ....	66
4.7.5 MLD snooping query configuration. ....	67
4.8 ACL configuration. ....	67
4.8.1 Time Range configuration. ....	67
4.8.2 Numeric ACL. ....	68
4.8.2.1 Standard numeric ACL. ....	68
4.8.2.2 Extended numeric ACL. ....	69
4.8.2.3 Delete Numeric ACL. ....	70
4.8.3 Name ACL. ....	71
4.8.3.1 Standard name ACL. ....	71
4.8.3.2 Extended name ACL. ....	71
4.8.3.3 Delete Name ACL. ....	73
4.8.4 Firewall configuration. ....	74
4.8.5 Show ACL configuration. ....	74
4.8.5.1 Show access list. ....	74
4.8.5.2 Show firewall. ....	75
4.8.5.3 Show time range. ....	75
4.8.6 ACL binding configuration. ....	75
4.8.6.1 Attach ACL to port. ....	75
4.8.6.2 Show access group. ....	76
4.8.6.3 Clear PACL Statistic. ....	76
4.8.6.4 Attach ACL to vlan. ....	76
4.8.6.5 Show VACL configuration. ....	77
4.8.6.6 Clear vlan ACL statistic. ....	77
4.9 IPv6 ACL configuration. ....	77
4.9.1 IPv6 standard access-list configuration. ....	77
4.9.2 IPv6 name access-list configuration. ....	78
4.9.3 Show IPv6 access list. ....	78
4.9.4 Attach IPv6 ACL to port. ....	78
4.9.5 Attach IPv6 ACL to vlan. ....	79
4.10 AM configuration. ....	79
4.10.1 AM global configuration. ....	79
4.10.1.1 Enable/Disable AM. ....	79
4.10.2 AM port configuration. ....	80
4.10.2.1 Enable/Disable AM port. ....	80
4.10.2.2 AM IP-Pool configuration. ....	81
4.10.2.3 AM MAC-IP-Poll configuration. ....	81
4.10.3 Show AM port configuration. ....	81

---

4.10.3.1 Show AM port configuration. ....	81
4.10.3.2 Clear port configuration.....	82
4.11 Port channel configuration.....	82
4.11.1 LACP port group configuration. ....	82
4.11.2 Delete port group.....	83
4.11.3 Show port group info.....	83
4.11.4 Show interface port-channel. ....	83
4.11.5 Add member port. ....	84
4.11.6 Del member port.....	84
4.11.7 Set LACP port priority. ....	84
4.11.8 Set LACP system priority.....	85
4.12 DHCP configuration. ....	85
4.12.1 DHCP management.....	85
4.12.1.1 Enable DHCP.....	86
4.12.2 DHCP server configuration. ....	86
4.12.2.1 Dynamic pool configuration. ....	86
4.12.2.2 Manual DHCP IP pool configuration. ....	89
4.12.2.3 Address pool name configuration. ....	90
4.12.2.4 DHCP packet statistics.....	90
4.12.3 DHCP relay configuration. ....	91
4.12.4 DHCP debugging. ....	91
4.12.4.1 Delete record.....	92
4.12.4.2 Show IP-MAC binding.....	93
4.12.4.3 Show conflict-logging. ....	93
4.13 DHCP Snooping configuration.....	93
4.13.1 DHCP Snooping global configuration.....	93
4.13.1.1 Enable/Disable DHCP Snooping.....	94
4.13.1.2 DHCP Snooping binding configuration. ....	94
4.13.1.3 DHCP Snooping binding user configuration. ....	94
4.13.1.4 DHCP Snooping action count config.....	95
4.13.1.5 DHCP Snooping limit-rate config.....	95
4.13.1.6 DHCP Snooping helper-server config.....	95
4.13.2 DHCP Snooping port configuration. ....	96
4.13.2.1 Enable/Disable DHCP Snooping binding dot1x. ....	96
4.13.2.2 Enable/Disable DHCP Snooping binding user. ....	96
4.13.2.3 Enable/Disable DHCP Snooping trust.....	97
4.13.2.4 DHCP Snooping action config. ....	97
4.13.3 Show DHCP Snooping configuration. ....	98
4.14 SNTP configuration. ....	98
4.14.1 SNTP server configuration.....	98
4.14.2 Request interval configuration.....	99
4.14.3 Time difference configuration. ....	99
4.14.4 Show SNTP.....	99
4.15 NTP configuration.....	100

---

4.15.1 NTP global configuration.....	100
4.15.1.1 NTP global switch configuration. ....	100
4.15.1.2 NTP server configuration. ....	100
4.15.1.3 NTP broadcast or multicast address count configuration. ....	101
4.15.1.4 NTP access group configuration. ....	101
4.15.1.5 NTP authenticate configuration. ....	101
4.15.2 NTP interface configuration. ....	102
4.15.2.1 NTP interface switch configuration.....	102
4.15.3 NTP configuration display. ....	102
4.15.3.1 NTP status display. ....	103
4.16 QoS configuration.....	103
4.16.1 QoS port configuration. ....	103
4.16.1.1 QoS port trust state configuration.....	104
4.16.1.2 QoS port cos parameters configuration.....	104
4.16.1.3 QoS port select queue schedule algorithm configuration. ....	105
4.16.1.4 QoS port WRR algorithm queue weight configuration. ....	105
4.16.1.5 QoS port WDRR algorithm queue weight configuration. ....	106
4.16.1.6 QoS port queue bandwidth configuration.....	107
4.16.1.7 QoS service policy configuration. ....	107
4.16.2 QoS class-map configuration. ....	108
4.16.2.1 Class map-configuration. ....	108
4.16.2.2 Classification criteria configuration.....	108
4.16.3 QoS policy-map configuration. ....	109
4.16.3.1 Policy-map configuration. ....	109
4.16.3.2 Class-map use to policy-map configuration.....	109
4.16.4 QoS policy-class-map configuration.....	109
4.16.4.1 Policy-class-map accounting configuration.....	110
4.16.4.2 Aggregate policy configuration.....	110
4.16.4.3 Policy-class-map policy configuration.....	110
4.16.4.4 Policy-class-map set configuration.....	111
4.16.5 QoS mapping configuration. ....	112
4.16.5.1 COS-to-IntP mapping. ....	112
4.16.5.2 COS-to-IntP mapping. ....	113
4.16.5.3 DSCP-to-DSCP mapping.....	113
4.16.5.4 DSCP-to-IntP mapping.....	114
4.16.5.5 DSCP-to-DP mapping. ....	114
4.16.6 QoS aggregate policy configuration. ....	115
4.16.7 QoS service policy configuration. ....	116
4.17 L3 forward configuration.....	116
4.17.1 IP route Aggregation configuration. ....	116
4.17.1.1 Route aggregate configuration. ....	116
4.17.2 ARP configuration. ....	117
4.17.2.1 ARP configuration. ....	117
4.17.2.2 Clear ARP cache.....	117

---

4.17.2.3 Show ARP .....	118
4.17.2.4 Proxy ARP configuration .....	118
4.17.3 Gratuitous ARP config. ....	118
4.17.3.1 Gratuitous-ARP interval time configuration .....	119
4.17.3.2 Interface Gratuitous-ARP interval time configuration .....	119
4.17.3.3 Show Gratuitous-ARP configuration .....	119
4.17.4 ARP protection configuration .....	120
4.17.4.1 ARP protection configuration .....	120
4.17.4.2 ANTI-ARPSCAN configuration .....	121
4.17.5 Show IP Traffic .....	124
4.18 Route configuration .....	125
4.18.1 Static route configuration .....	125
4.18.1.1 Static route configuration .....	126
4.18.2 RIP configuration .....	126
4.18.2.1 Enable RIP .....	127
4.18.2.2 Clear IP Route configuration .....	127
4.18.2.3 Default configuration .....	128
4.18.2.4 Distance configuration .....	128
4.18.2.5 Distribute-list configuration .....	128
4.18.2.6 Interface RIP configuration .....	129
4.18.2.7 Key or key-chain configuration .....	129
4.18.2.8 Send-LifeTime configuration .....	130
4.18.2.9 Accept-LiftTime configuration .....	130
4.18.2.10 RIP maximum-prefix .....	131
4.18.2.11 Neighbor configuration .....	131
4.18.2.12 Network configuration .....	131
4.18.2.13 Offset-list configuration .....	131
4.18.2.14 Passive interface configuration .....	132
4.18.2.15 Receive buffer size configuration .....	132
4.18.2.16 Receive route configuration .....	132
4.18.2.17 RIP route configuration .....	133
4.18.2.18 RIP timer configuration .....	133
4.18.2.19 Version configuration .....	133
4.18.3 OSPF configuration .....	134
4.18.3.1 OSPF enable .....	134
4.18.3.2 OSPF area configuration .....	135
4.18.3.3 OSPF interface configuration .....	136
4.18.3.4 Other parameters configuration .....	137
4.18.4 IP Prefix configuration .....	138
4.18.4.1 IP prefix list .....	138
4.18.4.2 IP prefix description .....	138
4.18.4.3 Show IP prefix-list .....	139
4.18.5 Show IP route .....	139
4.19 IPv6 Route configuration .....	139



---

4.19.1 IPv6 configuration. ....	139
4.19.1.1 IPv6 basic configuration.....	140
4.19.1.2 IPv6 ND configuration. ....	140
4.19.1.3 Show IPv6 neighbor.....	140
4.19.2 Show IPv6 route. ....	141
4.19.2.1 Show IPv6 route database. ....	141
4.19.2.2 Show IPv6 NSM route.....	141
4.19.2.3 Show IPv6 FIB.....	141
4.19.2.4 Show IPv6 route statistics.....	142
4.20 Multicast protocol configuration.....	142
4.20.1 DCSCM configuration.....	142
4.20.1.1 DCSCM Source-control enable/disable configuration.....	143
4.20.1.2 DCSCM destination-control enable/disable configuration. ....	143
4.20.1.3 DCSCM Source-control access-group configuration.....	144
4.20.1.4 DCSCM destination-control access-group configuration. ....	144
4.20.1.5 DCSCM destination-control access-group configuration(SIP).....	144
4.20.1.6 DCSCM destination-control access-group configuration(vMAC). ....	145
4.20.1.7 Multicast policy configuration. ....	145
4.20.1.8 ACL multicast source control.....	145
4.20.2 IGMP configuration. ....	146
4.20.2.1 Access-group and immediate leave configuration. ....	146
4.20.2.2 IGMP query-interval configuration.....	147
4.20.2.3 Max response-time and timeout configuration. ....	147
4.20.2.4 Limit and Version configuration.....	148
4.20.2.5 IGMP Join Group configuration. ....	148
4.20.2.6 IGMP Static Group configuration. ....	149
4.21 IPv6 Multicast protocol configuration.....	149
4.21.1 MLD configuration. ....	149
4.21.1.1 MLD access-group and immediate leave configuration.....	149
4.21.1.2 MLD query-interval configuration.....	150
4.21.1.3 MLD max response-time and timeout configuration.....	150
4.21.1.4 MLD Limit and Version configuration. ....	151
4.21.1.5 MLD Join Group configuration. ....	151
4.21.1.6 MLD Static Group configuration.....	152
4.22 VRRP configuration.....	152
4.22.1 VRRP set.....	152
4.22.1.1 Create VRRP ID.....	153
4.22.1.2 VRRP virtual IP configuration.....	153
4.22.1.3 VRRP interface.....	153
4.22.1.4 VRRP enable.....	154
4.22.1.5 VRRP preempt. ....	154
4.22.1.6 VRRP priority. ....	154
4.22.1.7 VRRP interval.....	155
4.22.1.8 VRRP circuit.....	155

---

4.22.2 Show VRRP information. ....	155
4.23 Spanning- tree configuration.....	156
4.23.1 Spanning-tree field configuration. ....	156
4.23.1.1 Instance configuration. ....	156
4.23.1.2 Field name configuration. ....	156
4.23.1.3 Revision-level configuration. ....	157
4.23.2 Spanning-tree Port configuration. ....	157
4.23.2.1 PortFast configuration. ....	158
4.23.2.2 Port priority configuration.....	158
4.23.2.3 Port cost configuration. ....	159
4.23.2.4 Spanning-tree port mode. ....	159
4.23.2.5 Link-type configuration. ....	159
4.23.2.6 Spanning-tree agreement port configuration. ....	160
4.23.3 Spanning-tree global configuration.....	161
4.23.3.1 Spanning-tree global agreement port configuration.....	161
4.23.3.2 Forward-time configuration.....	161
4.23.3.3 Hello-time configuration. ....	162
4.23.3.4 Max age time configuration. ....	162
4.23.3.5 Max hop time configuration. ....	162
4.23.3.6 Spanning tree mode configuration.....	163
4.23.3.7 Spanning tree cost-format configuration.....	163
4.23.3.8 Priority configuration.....	163
4.23.4 Show Spanning-tree. ....	164
4.23.4.1 Instance information. ....	164
4.23.4.2 Revision-Level information. ....	164
4.24 MRPP configuration. ....	165
4.24.1 MRPP global configuration. ....	165
4.24.1.1 MRPP global switch configuration.....	165
4.24.1.2 MRPP poll time configuration.....	166
4.24.1.3 MRPP domain id configuration. ....	166
4.24.2 MRPP port configuration.....	166
4.24.2.1 MRPP port property configuration. ....	166
4.24.3 MRPP domain configuration.....	167
4.24.3.1 MRPP control vlan config. ....	167
4.24.3.2 MRPP node mode config.....	168
4.24.3.3 MRPP hello timer config. ....	168
4.24.3.4 MRPP fail timer config.....	168
4.24.3.5 MRPP domain switch config.....	169
4.24.4 MRPP configuration display.....	169
4.24.4.1 MRPP statistics display. ....	170
4.24.4.2 MRPP display. ....	170
4.24.4.3 Clear MRPP statistics.....	170
4.25 ULPP configuration. ....	170
4.25.1 ULPP global configuration. ....	171

---

4.25.1.1 ULPP group configuration. ....	171
4.25.2 ULPP port configuration. ....	171
4.25.2.1 ULPP port property configuration. ....	171
4.25.3 ULPP group configuration. ....	172
4.25.3.1 ULPP description configuration. ....	172
4.25.3.2 ULPP group property configuration. ....	172
4.25.4 ULPP configuration display. ....	173
4.25.4.1 ULPP group configuration display. ....	173
4.25.4.2 ULPP port statistics display. ....	173
4.25.4.3 ULPP port property display. ....	174
4.25.4.4 ULPP port statistics clear. ....	174
4.26 ULSM configuration. ....	174
4.26.1 ULSM global configuration. ....	174
4.26.1.1 ULSM group configuration. ....	175
4.26.2 ULSM port configuration. ....	175
4.26.2.1 ULSM port property configuration. ....	175
4.26.3 ULSM configuration display. ....	176
4.26.3.1 ULSM display. ....	176
4.27 Cluster basic configuration. ....	176
4.27.1 Cluster configuration. ....	176
4.27.2 Cluster candidate information. ....	177
4.27.3 Cluster member information. ....	177
4.27.4 Cluster member configuration. ....	177
4.27.5 Cluster member auto configuration. ....	178
4.27.6 Cluster member reset. ....	178
4.27.7 Cluster topology configuration. ....	178
4.27.8 Cluster topology information. ....	178
4.28 Authentication configuration. ....	179
4.28.1 RADIUS client configuration. ....	179
4.28.1.1 RADIUS global configuration. ....	179
4.28.1.2 RADIUS authentication configuration. ....	180
4.28.1.3 RADIUS accounting configuration. ....	180
4.28.2 TACACS server configuration. ....	181
4.28.2.1 TACACS global configuration. ....	181
4.28.2.2 TACACS server host configuration. ....	181
4.28.3 802.1x configuration. ....	182
4.28.3.1 802.1x Global configuration. ....	182
4.28.3.2 802.1x port authentication configuration. ....	183
4.28.3.3 802.1x port MAC configuration list. ....	184
4.28.3.4 802.1x port status list. ....	184
4.28.4 MAB configuration. ....	184
4.28.4.1 MAB ENABLE configuration. ....	184
4.28.4.2 MAB Authentication configuration. ....	185
4.28.4.3 MAB parameter configuration. ....	185

---

4.28.4.4 MAB show. ....	186
4.29 PoE Config. ....	186
4.29.1 PoE global config. ....	186
4.29.1.1 PoE global config .....	186
4.29.2 PoE port config. ....	187
4.29.2.1 PoE port config .....	187
4.30 DOS attack protection configuration. ....	188
4.30.1 Source IP equal destination IP DOS attack protection configuration. ....	188
4.30.2 Source port equal destination port DOS attack protection configuration. ....	189
4.30.3 TCP DOS attacks on invalid flags configuration. ....	189
4.30.4 ICMP DOS attack protection configuration. ....	190
4.30.5 ICMP packet-size configuration. ....	190
4.30.6 First fragment IP packet DOS attack protection configuration. ....	191
4.31 SSL config. ....	191
4.31.1 IP HTTP server configuration. ....	192
4.31.2 SSL global configuration. ....	192
4.31.3 SSL server monitor port configuration. ....	192
4.31.4 SSL secure-ciphersuite configuration. ....	192
4.32 sFLOW configuration. ....	193
4.32.1 sFLOW collector global address configuration. ....	193
4.32.2 sFLOW collector port address configuration. ....	194
4.32.3 sFLOW agent address configuration. ....	194
4.32.4 sFLOW priority configuration. ....	194
4.32.5 sFLOW header length configuration. ....	194
4.32.6 sFLOW data length configuration. ....	195
4.32.7 sFLOW rate configuration. ....	195
4.32.8 sFLOW counter interval configuration. ....	195
4.32.9 sFLOW analyzer configuration. ....	196
4.33 IPv6 security ra configuration. ....	196
4.33.1 IPv6 security ra global configuration. ....	196
4.33.2 IPv6 security ra port configuration. ....	196
4.33.3 Show IPv6 security ra. ....	197
4.34 Device log message. ....	197
4.34.1 Show device log message in buffer. ....	197
4.34.2 Show logging flash. ....	198
4.34.3 Clear logging in logbuff channel. ....	198
<b>Appendix: Technical Specifications .....</b>	<b>199</b>

# **Chapter 1 Product Introduction**

Congratulations on your purchasing of the Ethernet Switch. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

## **1.1 Product Overshow**

This is a new generation designed for high security and high performance network the second layer switch. Provides twenty-four 10/100/1000Mbps self-adaption RJ45 port, plus four 10 Gigabit --1000/10000Mbps SFP+ optical port, it can be used to link bandwidth higher upstream equipment. Using store-and-forward technology, combined with dynamic memory allocation. Ensure bandwidth effective allocation to each port. Special design is a flow control. It can avoid packet loss effectively when nodes in the sending and receiving data. Built-in high reliability, design for wide voltage input application power supply, even if the voltage is not stable of power grid, also can guarantee the equipment can work normally.

The Switch is easy to install and use; It requires no configuration and installation; It is a great selection for expanding office network.

## **1.2 Features**

- Supports IEEE 802.3, IEEE 802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3az.
- Integrated High-Performance Cortex-A9 processor.
- Supports MAC address auto-learning and auto-aging.
- Twenty-four 10/100/1000Mbps self-adaption RJ45 port, plus four 10 gigabit port --- 10/100/1000/10000Mbps SFP+ optical port, it can be used to link bandwidth higher upstream equipment.
- Store and forward mode operates.
- LED indicators for monitoring power, link/activity.
- Support QoS, port mirroring, link aggregation protocol.
- 19 inches full metal iron shell and internal power adapter design, suitable for rack installation.

## **1.3 Package Contents**

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One 24-Port 10/100/1000Mbps + 4-Port 10 Gigabit Web Smart Ethernet Switch
- One set of installation components
- One AC power cord
- One User Manual

---

## **Chapter 2 External Component Description**

### **2.1 Front Panel**

The front panel of the Switch consists of series of LED indicators, 24 x 10/100/1000Mbps RJ-45 ports, 4 x 1000/10000Mbps SFP+ ports, 1 Console port, A reset button, A series of LED lights:



Figure 1 - Front Panel

#### **10/100/1000Mbps RJ-45 ports (1~24):**

Designed to connect to the device with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding Link LED.

#### **SFP+ ports (25S, 26S, 27S, 28S):**

Designed to install the SFP+ module and connect to the device with a bandwidth of 1000Mbps or 10000Mbps. Each has a corresponding Link/Act (1000M and 10G) LED.

#### **Control port (Console):**

It is used to connect a computer or terminal serial implementation of monitoring and configuring the switch.

#### **Reset key (Reset):**

Keep the device is turned on and press the button for about 4 seconds. The system restore the factory default settings.

#### **LED indicators:**

The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.

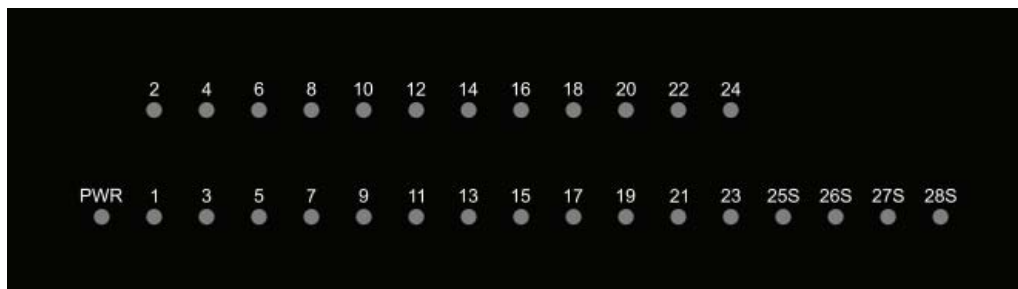


Figure 2 - LED Indicators

The following chart shows the LED indicators of the Switch along with explanation of each indicator.

LED	COLOR	STATUS	STATUS DESCRIPTION
PWR	Green	On	Power On
		Off	Power Off
1~28LED	Green	On	A device is connected to the port
		Off	A device is disconnected to the port
		Flashing	Sending or receiving data

## 2.2 Rear Panel

The rear panel of the Switch contains AC power connector shown as below.



Figure 3 - Rear Panel

### **AC Power Connector:**

Power is supplied through an external AC power adapter. It supports AC 100~240V, 50/60Hz.

### **Grounding Terminal:**

Located on the left side of the power supply connector, use wire grounded to prevent electric shock.

---

## **Chapter 3 Installing and Connecting the Switch**

This part describes how to install your Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

### **3.1 Installation**

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

#### **3.1.1 Desktop Installation**

Sometimes users are not equipped with the 19-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

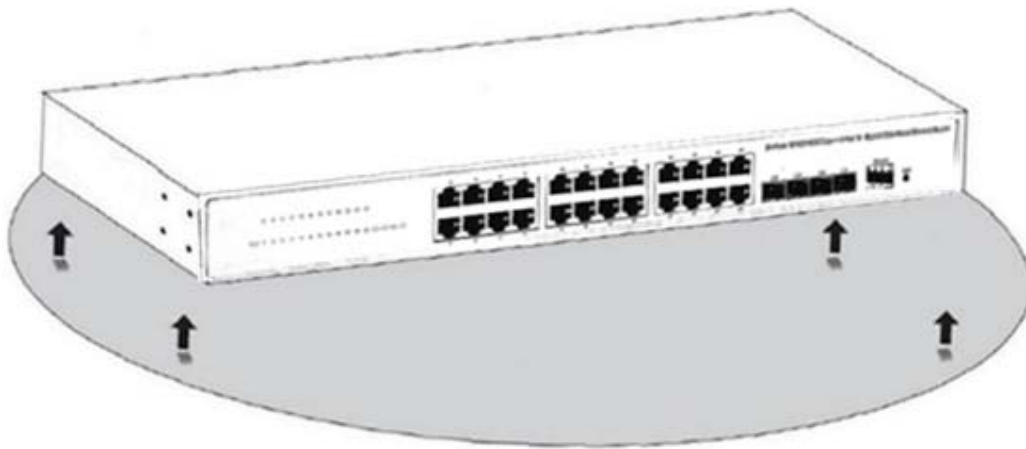


Figure 4 - Desktop installation

#### **3.1.2 Rack-mountable Installation in 19-inch Cabinet**

The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:



- 
- a. attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

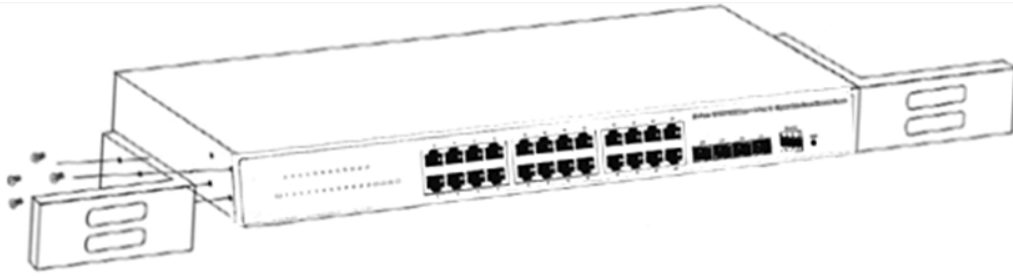


Figure 5 - Attaching Brackets

- b. use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

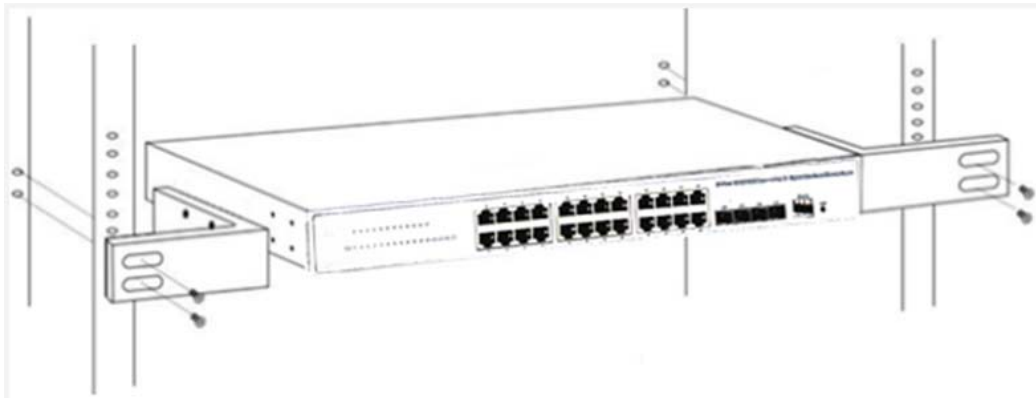


Figure 6 - Mounting Switch

### 3.1.3 Power on the Switch

The Switch is powered on by the AC 100~240V 50/60Hz internal high-performance power supply. Please follow the next tips to connect:

#### **AC Electrical Outlet:**

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

#### **AC Power Cord Connection:**

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

### 3.2 Connect Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please

---

connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the Link/ACT status indicator lights corresponding ports of the Switch.



Figure 7 - Connect Computer (NIC) to the Switch

### 3.3 How to Login the Switch

As the Switch provides Web-based management login, you can configure your computer's IP address manually to log on to the Switch. The default settings of the Switch are shown below.

Parameter	Default Value
Default IP address	192.168.2.1
Default user name	admin
Default password	admin

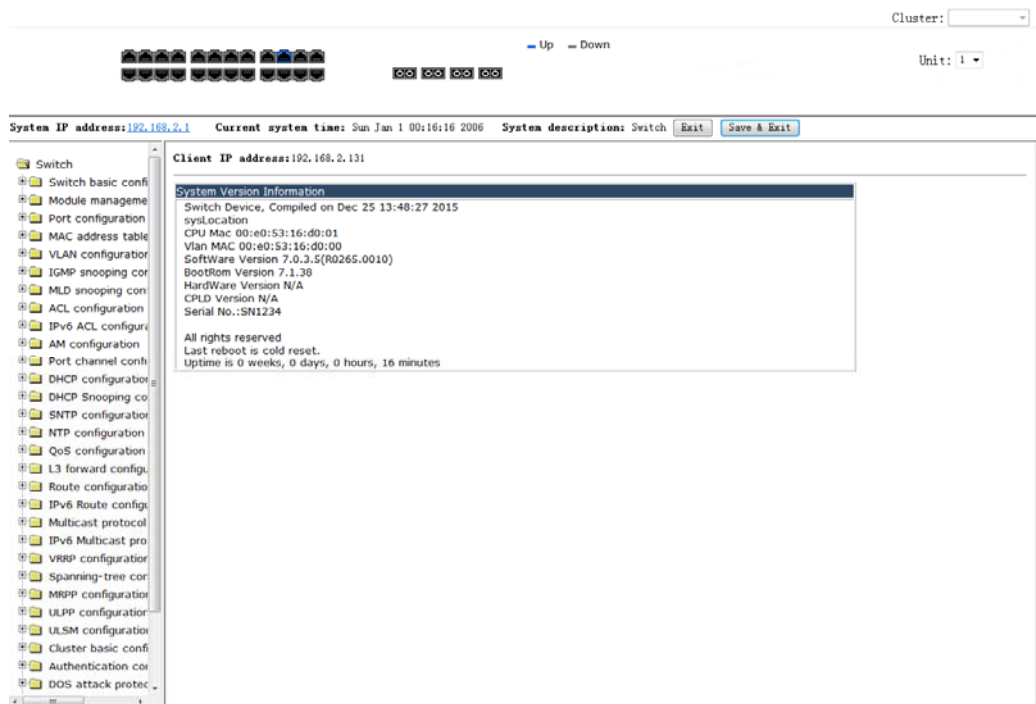
You can log on to the welcome window of the Switch through following steps:

- Connect the Switch with the computer NIC interface.
- Power on the Switch.
- Check whether the IP address of the computer is within this network segment: 192.168.2.xxx ("xxx" ranges 2~254), for example, 192.168.2.100.
- Open the browser, and enter <http://192.168.2.1> and then press "Enter". The Switch login window appears, as shown below.

A screenshot of a web-based login interface for a device labeled "FR-S3028PETF-C". The interface has a grey background. At the top, the device name is displayed in a dark grey box. Below it, there are two input fields: "Username" with the text "admin" and "Password" with five dots. A "login" button is located at the bottom right of the form.

- 
- 
- 
- 
- e.
- f. Enter the ID and Password (The default ID is **admin**. Password is **admin**), and then

click "OK" to log in to the Switch configuration window as below.



In the Web GUI, the left column shows the configuration menu and the rest of the screen area displays the configuration settings.

---

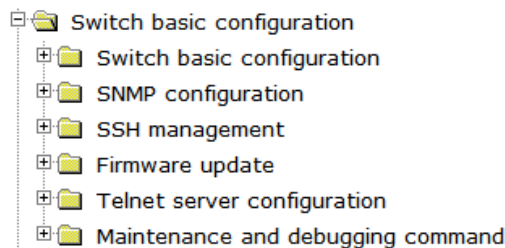
## **Chapter 4 Switch Configuration**

Switch configuration interface consists of 3 main areas, areas for the status bar at the top, the area on the left menu bar, right the main configuration window. Blue in the status bar indicates the RJ45 port connected, black corresponds to the RJ45 port means port is not connected. Select the different functions in the function menu bar, you can modify all settings in the main configuration window.

### **4.1 Switch basic configuration.**

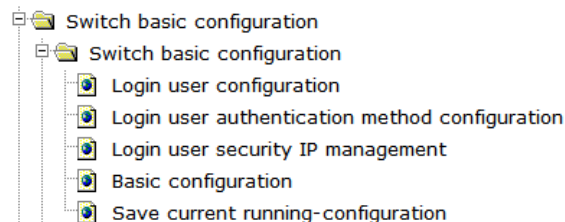
Choose **Switch basic configuration**, and the following page appears.

There are "Switch basic configuration", "SNMP configuration", "SSH management", "Firmware update", "Telnet server configuration", "Maintenance and debugging command", configuration web pages.



#### **4.1.1 Switch basic configuration.**

Choose **Switch basic configuration > Switch basic configuration**, and the following page appears. There are "Login user configuration", "Login user authentication method configuration", "Login user security IP management", "Basic configuration", "Save current running-configuration", configuration web pages.



##### **4.1.1.1 Login user configuration.**

Choose **Switch basic configuration > Switch basic configuration > Login user configuration**, and the following page appears. Enter the user name and password, and choose whether to encrypt the text, and sets the user priority, then you want to add or remove users.

Notes: User names and passwords between 1-32 characters. Priority between 1-15, defaults to 1.

Login username and password configuration	
User	<input type="text"/>
Password	<input type="text"/> <input type="checkbox"/> Encrypted text
Priority	<input type="text"/>
Operation	Remove ▼
<input type="button" value="Apply"/>	

User				
User name	Password	State	Priority	
admin	admin	Plain text	15	

#### 4.1.1.2 Login user authentication method configuration.

Choose **Switch basic configuration > Switch basic configuration > Login user authentication method configuration**, and the following page appears. Set the login and authentication methods, or to restore the default.

Login methods including Console, Vty, WEB, authentication methods. Authentication method including Local, RADIUS, Tacacs.

Login user authentication method configuration	
Login method	Console ▼
Authentication method1	None ▼
Authentication method2	None ▼
Authentication method3	None ▼
<input type="button" value="Apply"/>	<input type="button" value="Default"/>

Login user authentication method				
Login method	Authentication method1	Authentication method2	Authentication method3	
console	None	None	None	None
vty	local	None	None	None
web	local	None	None	None

#### 4.1.1.3 Login user security IP management.

Choose **Switch basic configuration > Switch basic configuration > Login user security IP management**, and the following page appears. Here you can add or delete an user's login security IP. In the user access control list settings, add or remove the Ipv4/Ipv6 Security address.

Login user Security IP Set	
Security IP address	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Login access control list set	
Ipv4 access control list ▼	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Login user security IPv4 list
end of security IPv4
Login user security IPv6 list
end of security IPv6
Login Ipv4 access control list
end of ipv4 access list
Login Ipv6 access control list
end of ipv6 access list

#### 4.1.1.4 Basic configuration.

Choose **Switch basic configuration > Switch basic configuration > Basic configuration**, and the following page appears. You can change the time, the switch name, configure the exec timeout.

Basic clock configuration	
HH:MM:SS	<input type="text"/>
YYYY.MM.DD	<input type="text"/>
<input type="button" value="Apply"/>	

Configure exec timeout	
Timeout(minute)	<input type="text"/>
Timeout(second)	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

Switch name configuration	
Switch name	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

#### 4.1.1.5 Save current running-configuration.

Choose **Switch basic configuration > Switch basic configuration > Save current running-configuration**, and the following page appears. These three function provide to save current running-configuration, reboot with restore configuration to default, and reboot with save current configuration or not.

---

Save current running-configuration

Apply

Reboot with the default configuration

Apply

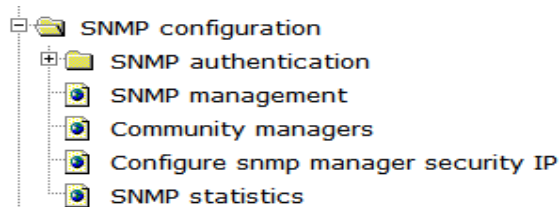
Save current configuration before reboot?

Yes ▾

Apply

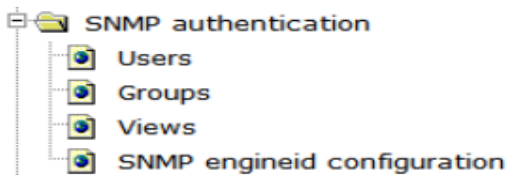
### 4.1.2 SNMP configuration.

Choose **Switch basic configuration > SNMP configuration**, and the following page appears. Changing SNMP authentication parameters must start SNMP function first, go to "SNMP Management" page to change item "SNMP Agent state" to open. There are "SNMP authentication", "SNMP management", "Community managers", "Configure snmp manager security IP", "SNMP statistics", configuration web pages.



#### 4.1.2.1 SNMP authentication.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication**, and the following page appears. There are "Users", "Groups", "show", "SNMP engineid configuration", configuration web pages.



##### 4.1.2.1.1 Users.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication > Users**, and the following page appears. Here you can set the SNMP user name, SNMP group, and the security level, the IPv4 and IPv6 access control lists. Security level including ,no certification and no encryption, authentication without encryption, authentication with encryption.

Note: the Authentication password and Privacy password in 8-32 characters.

Note: the SNMP User name and SNMP Group in 1-32 characters.

Users	
SNMP username	<input type="text"/>
SNMP group	<input type="text"/>
Security level	noAuthNoPriv ▼
Authentication protocol:	MD5 ▼
Authentication password:	<input type="text"/>
Privacy protocol:	DES ▼
Privacy password:	<input type="text"/>
Ipv4 access control list	<input type="text"/>
Ipv6 access control list	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.1.2.1.2 Groups.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication > Groups**, and the following page appears. Set the security level, read SNMP shows, write SNMP shows, notifies the SNMP show operation.

Groups	
SNMP group	<input type="text"/>
Security level	noAuthNoPriv ▼
Read SNMP view	<input type="text"/>
Write SNMP view	<input type="text"/>
Notify SNMP view	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.1.2.1.3 shows.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication > shows**, and the following page appears. This page allows to add or remove a SNMP policy. Fill the show item and OID to include or exclude the corresponding MIB.

Views	
SNMP view	<input type="text"/>
OID	<input type="text"/>
Type:	Include ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

SNMP view	OID	Type
v1defaultviewname	1.0.	Include
v1defaultviewname	1.2.	Include
v1defaultviewname	1.3.	Include

#### 4.1.2.1.4 SNMP engineid configuration.

Choose **Switch basic configuration > SNMP configuration > SNMP authentication >**



**SNMP engineid configuration**, and the following page appears. If not necessary, don't change the default engineid value.

SNMP engineid configuration	
Engineid	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	
Engineid	
18c300e05316d001	

#### 4.1.2.2 SNMP management.

Choose **Switch basic configuration > SNMP configuration > SNMP management**, and the following page appears. You can open or close SNMP, RMON, Trap, Security IP state function.

SNMP management	
SNMP Agent state	Open ▾
RMON state	Open ▾
Trap state	Open ▾
SecurityIP state	Open ▾
<input type="button" value="Apply"/>	

#### 4.1.2.3 Community managers.

Choose **Switch basic configuration > SNMP configuration > Community managers**, and the following page appears. At this page, you can configure the community string for different priority, and set the Trap receiver address, community string, version, security level for trap message.

Community managers	
Community string	<input type="text"/>
Access priority	Read only ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Community string Access priority

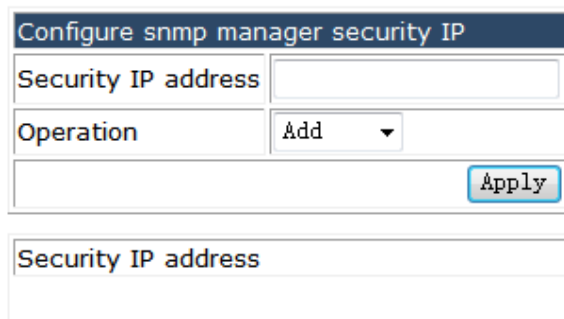
TRAP manager configuration	
Trap receiver	<input type="text"/>
Community string	<input type="text"/>
Version	1 ▾
Security level	noAuthNoPriv ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Trap receiver Community string Version Security level

---

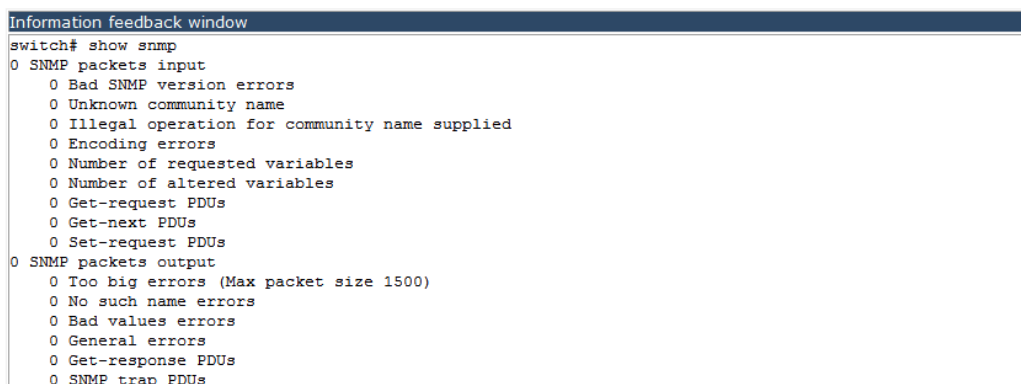
#### 4.1.2.4 Configure snmp manager security IP.

Choose **Switch basic configuration > SNMP configuration > Configure snmp manager security IP**, and the following page appears. You can add or remove Security IP address for SNMP management.



#### 4.1.2.5 SNMP statistics.

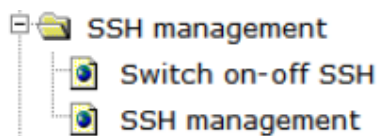
Choose **Switch basic configuration > SNMP configuration > SNMP statistics**, and the following page appears. From this window ,you can read the detail statistics message for SNMP.



```
switch# show snmp
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors (Max packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Get-response PDUs
  0 SNMP trap PDUs
```

#### 4.1.3 SSH management.

Choose **Switch basic configuration > SSH management**, and the following page appears. There are "Switch on-off SSH", "SSH management", configuration web pages.



##### 4.1.3.1 Switch on-off SSH.

Choose **Switch basic configuration > SSH management > Switch on-off SSH**, and the following page appears. Choose open or close to turn on-off SSH function.

Switch on-off SSH

Switch on-off SSH

Open ▾

Apply

### 4.1.3.2 SSH management.

Choose **Switch basic configuration > SSH management > SSH management**, and the following page appears. You can set the SSH timeout, SSH re-certification number and create a SHH RSA keys.

SSH timeout management

SSH timeout

Operation

Configuration ▾

Apply

SSH reauthentication management

SSH reauthentication

Operation

Configuration ▾

Apply

Create SSH RSA key

SSH RSA key

1024

Apply

SSH timeout

180

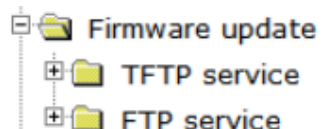
SSH reauthentication

3

Show SSH Server's State			
Num	Version	Status	SSH username

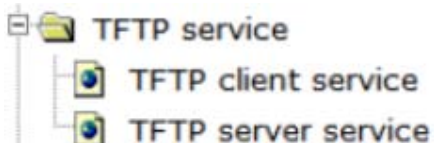
### 4.1.4 Firmware update.

Choose **Switch basic configuration > Firmware update**, and the following page appears. There are "TFTP service", "FTP service", configuration web pages.



#### 4.1.4.1 TFTP service.

Choose **Switch basic configuration > Firmware update > TFTP service**, and the following page appears. There are "TFTP client service", "TFTP server service", configuration web pages.



##### 4.1.4.1.1 TFTP client service.

Choose **Switch basic configuration > Firmware update > TFTP service > TFTP client service**, and the following page appears. You can set the TFTP client service.

TFTP client service	
Server IP address	<input type="text"/>
Local file name	<input type="text"/>
Server file name	<input type="text"/>
Operation type	Upload ▾
Transmission type	binary ▾
<input type="button" value="Apply"/>	

#### 4.1.4.1.2 TFTP server service.

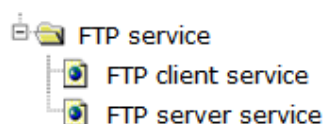
Choose **Switch basic configuration > Firmware update > TFTP service > TFTP server service**, and the following page appears. You can open or close the TFTP server function, set timeout and retransmit times value, or reset these parameters to factory default.

TFTP server service	
TFTP Server state	Close ▾
TFTP Timeout	600
TFTP Retransmit times	5
Operation	Configuration ▾
<input type="button" value="Apply"/>	

TFTP Server state	TFTP Timeout	TFTP Retransmit times
Close	600	5

#### 4.1.4.2 FTP service.

Choose **Switch basic configuration > Firmware update > FTP service**, and the following page appears. There are "FTP client service", "FTP server service", configuration web pages.



##### 4.1.4.2.1 FTP client service.

Choose **Switch basic configuration > Firmware update > FTP service > FTP client service**, and the following page appears. Fill the IP address, User name, Password of the FTP server, setting the local file name and server file name, then you can upload or download the file to the FTP server. Also you can select the transmit type using binary or ASCII.

FTP client service	
Server IP address	<input type="text"/>
User	<input type="text"/>
Password	<input type="text"/>
Local file name	<input type="text"/>
Server file name	<input type="text"/>
Operation type	Upload ▾
Transmission type	binary ▾
<input type="button" value="Apply"/>	

#### 4.1.4.2.2 FTP server service.

Choose **Switch basic configuration > Firmware update > FTP service > FTP server service**, and the following page appears. You can choose open or close the FTP server function. Also you can set timeout value, user name, password, and plain text or encrypted text display the password for the FTP server.

FTP server service	
FTP server State	Close ▾
FTP Timeout	600
Operation	Configuration ▾
<input type="button" value="Apply"/>	

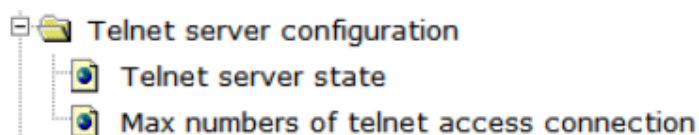
FTP server State	FTP Timeout
Close	600

FTP user name and password setting	
User	<input type="text"/>
Password	<input type="text"/>
State	Plain text ▾
Operation type	Add ▾
<input type="button" value="Apply"/>	

User name	Password	State
-----------	----------	-------

#### 4.1.5 Telnet server configuration.

Choose **Switch basic configuration > Telnet server configuration**, and the following page appears. There are "Telnet server state", "Max numbers of telnet access connection", configuration web pages.



---

#### 4.1.5.1 Telnet server state.

Choose **Switch basic configuration > Telnet server configuration > Telnet server state**, and the following page appears. You can open or close the Telnet Server.

Telnet server state	
Telnet server state	Open ▼
<div>Apply</div>	

#### 4.1.5.2 Max number of telnet access connection.

Choose **Switch basic configuration > Telnet server configuration > Max number of telnet access connection**, and the following page appears. Set Max number of Telnet access. The default number is 5.

Max numbers of telnet access connection	
Telnet access connection number	<input type="text"/>
Operation	Configuration ▼
<div>Apply</div>	

Information feedback window	
Telnet access connection number	5

#### 4.1.6 Maintenance and debugging command.

Choose **Switch basic configuration > Maintenance and debugging command**, and the following page appears. There are "Debug command", "show clock", "show cpu usage", "show memory usage", "show flash", "show running-config", "show switchport interface", "show tcp", "show udp", "show telnet login", "show version", configuration web pages.

☞ Maintenance and debugging command

- Debug command
- show clock
- show cpu usage
- show memory usage
- show flash
- show running-config
- show switchport interface
- show tcp
- show udp
- show telnet login
- show version

---

#### 4.1.6.1 Debug command.

Choose **Switch basic configuration > Maintenance and debugging command > Debug command**, and the following page appears. You can add or remove the Host name and IP address to the list. And you can test the connectivity between switch and the destination host via ping or traceroute method..

Basic host configuration	
Host name	<input type="text"/>
IP address	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

PING	
Host name	<input type="text"/>
IP address	<input type="text"/>
<input type="button" value="Apply"/>	

Traceroute	
IP address	<input type="text"/>
Host name	<input type="text"/>
Hops	<input type="text"/>
timeout	<input type="text"/>
<input type="button" value="Apply"/>	

Host name	IP address
-----------	------------

#### 4.1.6.2 Show clock.

Choose **Switch basic configuration > Maintenance and debugging command > show clock**, and the following page appears. You can see the current time information of the device.

```
Information feedback window
switch# show clock
Current time is Sun Jan 01 05:55:54 2006
```

#### 4.1.6.3 Show cpu usage.

Choose **Switch basic configuration > Maintenance and debugging command > show cpu usage**, and the following page appears. You can see the CPU usage information of the device.

```
Information feedback window
switch# show cpu usage
Last 5 second CPU IDLE: 94%
Last 30 second CPU IDLE: 93%
Last 5 minute CPU IDLE: 93%
From running CPU IDLE: 93%
```

---

#### 4.1.6.4 Show cpu show memory usage.

Choose **Switch basic configuration > Maintenance and debugging command > show Memory usage**, and the following page appears. You can see the memory usage information of the device.

```
Information feedback window
switch# show memory usage
The memory total 512 MB , free 437805056 bytes , usage is 18.45%
```

#### 4.1.6.5 Show flash.

Choose **Switch basic configuration > Maintenance and debugging command > show flash**, and the following page appears. You can see the all the files store in the flash, and the flash usage of the device.

```
Information feedback window
switch# show flash
-rw-      1.7K      backupstartup.cfg
-rw-        4      board_web_language
-rw-     13.1M      nos.img
-rw-      1.0K      startup.cfg
Drive : flash:
Size:14.0M  Used:13.9M  Aavailable:64.0K  Use:100%
```

#### 4.1.6.6 Show running-config.

Choose **Switch basic configuration > Maintenance and debugging command > show running-config**, and the following page appears. You can see the running-configure information of the device.

```
Information feedback window
switch# show run
!
no service password-encryption
!
hostname switch
sysLocation FullRiver Industrial Area Economic Development Zone LiLing City HuNan Province China
sysContact 0731-2325 0117
!
authentication logging enable
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
```

#### 4.1.6.7 Show switchport interface.

Choose **Switch basic configuration > Maintenance and debugging command > show switchport interface**, and the following page appears. You can see all the ports and their type and mode information of device.



```
Information feedback window
switch# show switchport interface
Ethernet1/0/1
Type :Universal
Mode :Access
Port VID :1
Ethernet1/0/2
Type :Universal
Mode :Access
Port VID :1
Ethernet1/0/3
Type :Universal
Mode :Access
Port VID :1
Ethernet1/0/4
```

#### 4.1.6.8 Show tcp.

Choose **Switch basic configuration > Maintenance and debugging command > show tcp**, and the following page appears.You can see the current TCP connection information of the device.

Information feedback window						
switch# show tcp						
LocalAddress	LocalPort	ForeignAddress	ForeignPort	State	IF	VRF
192.168.2.1	80	192.168.2.22	49342	ESTABLISHED	0	0
127.0.0.1	2650	127.0.0.1	32862	ESTABLISHED	0	0
127.0.0.1	32862	127.0.0.1	2650	ESTABLISHED	0	0
0.0.0.0	6633	0.0.0.0	0	LISTEN	0	0
0.0.0.0	80	0.0.0.0	0	LISTEN	0	0
0.0.0.0	22	0.0.0.0	0	LISTEN	0	0
0.0.0.0	23	0.0.0.0	0	LISTEN	0	0
127.0.0.1	2650	0.0.0.0	0	LISTEN	0	0

#### 4.1.6.9 Show udp.

Choose **Switch basic configuration > Maintenance and debugging command > show udp**, and the following page appears.You can see the current UDP transmission information of the device.

Information feedback window				
switch# show udp				
LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	161	0.0.0.0	0	CLOSE
0.0.0.0	3071	0.0.0.0	0	CLOSE

#### 4.1.6.10 Show telnet login.

Choose **Switch basic configuration > Maintenance and debugging command > show telnet login**, and the following page appears.You can see the current client host logged in via telnet.

#### Information feedback window

```
switch# show telnet login
Authenticate login by local.
Login user:
```

### 4.1.6.11 Show version.

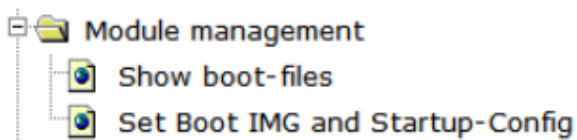
Choose **Switch basic configuration > Maintenance and debugging command > show version**, and the following page appears. You can see the detail version information of the device.

#### System Version Information

```
FR-S3028TF-C Device, Compiled on Feb 01 16:58:10 2016
sysLocation FullRiver Industrial Area Economic Development Zone LiLing City HuNan Province China
CPU Mac 00:e0:53:16:d0:01
Vlan MAC 00:e0:53:16:d0:00
SoftWare Version 7.0.3.5(R0265.0012)
BootRom Version 7.1.38
HardWare Version N/A
CPLD Version N/A
Serial No.:SN1234
Copyright (C) 2008-2016 by Liling FullRiver Electronic & Technology Limited
All rights reserved
Last reboot is warm reset.
Uptime is 0 weeks, 0 days, 6 hours, 26 minutes
```

## 4.2 Module management.

Choose **Module management**, and the following page appears. There are "Show boot-files", "Set Boot IMG and Startup-Config", configuration web pages.



### 4.2.1 Show boot-files.

Choose **Module management > Show boot-files**, and the following page appears. You can see the current boot file and configure file, also the next boot time files.

#### Information feedback window

```
Booted files on switch
The primary img file at the next boot time:      flash:/nos.img
The backup img file at the next boot time:       flash:/nos.img
Current booted img file:                         flash:/nos.img

The startup-config file at the next boot time:    NULL
Current booted startup-config file:              NULL
```

---

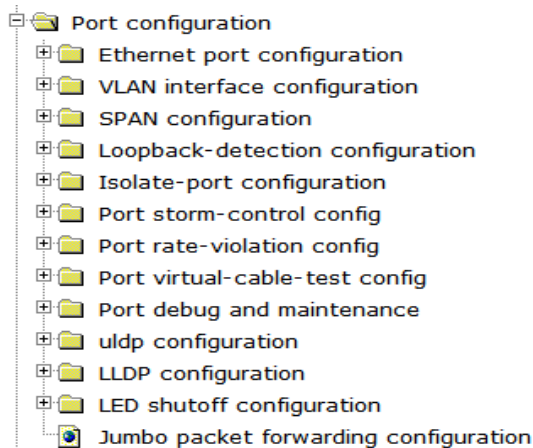
## 4.2.2 Set Boot IMG and Startup-Config.

Choose **Module management > Set Boot IMG and Startup-Config**, and the following page appears. You can specify the boot files and startup-config file for next boot time.

Set boot files in Active Master		
Primary IMG		Set
Backup IMG		Set
Startup-config		Set

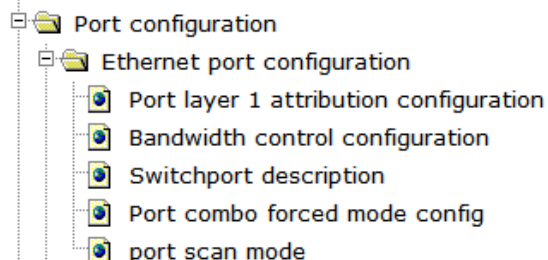
## 4.3 Port configuration.

Choose **Port configuration**, and the following page appears. There are "Ethernet port configuration", "VLAN interface configuration", "SPAN configuration", "Loopback-detection configuration", "Isolate-port configuration", "Port storm-control config", "Port rate-violation config", "Port virtual-cable-test config", "Port debug and maintenance", "uldp configuration", "LLDP configuration", "LED shutoff configuration", "Jumbo packet forwarding configuration", configuration web pages.



### 4.3.1 Ethernet port configuration.

Choose **Port configuration > Ethernet port configuration**, and the following page appears. There are "Port layer 1 attribution configuration", "Bandwidth control configuration", "Switchport description", "Port combo forced mode config", "Port scan mode", configuration web pages.



---

#### 4.3.1.1 Port layer 1 attribution configuration.

Choose **Port configuration > Ethernet port configuration > Port layer 1 attribution configuration**, and the following page appears. You can set the parameters for every port, and the Port List table display the configuration information for each port.

Port configuration		
Port	Ethernet1/0/1 ▾	
mdi	auto ▾	<input type="checkbox"/>
Admin status	no shutdown ▾	<input type="checkbox"/>
Speed/Duplex status	Auto ▾	<input type="checkbox"/>
Module type	auto-detected ▾	<input type="checkbox"/>
1000M Mode	▾	<input type="checkbox"/>
Fiber portMode	Auto ▾	<input type="checkbox"/>
Flow control status	Invalid flow control ▾	<input type="checkbox"/>
Loopback	no loopback ▾	<input type="checkbox"/>
<input type="button" value="Apply"/>		

Port-Specify the port to be configured.

mdi-Set the interface type for the port, auto means support automatic flip, across means support cross wire, normal means support straight-through line.

Admin status-Shutdown or no shutdown the port.

Speed/Duplex status-Set the speed and duplex mode including 10M/Half、 10M/Full、 100M/Half、 100M/Full、 1000M/Half、 1000M/Full and so on.

Module type-Set the 100M light module type supported by the switch including auto-detected, no-phy-integrated, phy-integrated, this parameter just for SFP+ optical port.

Fiber port Mode-Include auto and non negotiation mode.

Flow control status-Set valid or invalid flow control.

Loopback-Whether to configure loop detection function.

Port list								
Port	mdi	managementStatus	Speed	Mode	1000M Mode	Fiber portMode	Flow control	loopback
Ethernet1/0/1	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/2	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/3	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/4	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/5	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/6	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/7	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/8	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/9	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback
Ethernet1/0/10	auto	No Shutdown	auto	auto	NULL	Auto	Non flow control status	no loopback

#### 4.3.1.2 Bandwidth control configuration.

Choose **Port configuration > Ethernet port configuration > Bandwidth control configuration**, and the following page appears. You can limit the bandwidth rang 1-10000000Kb for each port divided for transmit and receive direction.

Bandwidth control configuration			
Port	Bandwidth control level	Control type	Operation
Ethernet1/0/1 ▼	<input type="text"/>	Transmit ▼	Configuration ▼

Port list		
Port	Ingress bandwidth threshold(Kb)	Engress bandwidth threshold(Kb)
Ethernet1/0/1	1000000	1000000
Ethernet1/0/2	1000000	1000000
Ethernet1/0/3	1000000	1000000
Ethernet1/0/4	1000000	1000000
Ethernet1/0/5	1000000	1000000
Ethernet1/0/6	1000000	1000000
Ethernet1/0/7	1000000	1000000
Ethernet1/0/8	1000000	1000000

#### 4.3.1.3 Switchport description.

Choose **Port configuration > Ethernet port configuration > Switchport description**, and the following page appears. You can set the description of the switch port.

Switchport description	
Port	Ethernet1/0/1 ▾
Description	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Port list	
Port	Description
Ethernet1/0/1	
Ethernet1/0/2	
Ethernet1/0/3	
Ethernet1/0/4	
Ethernet1/0/5	
Ethernet1/0/6	
Ethernet1/0/7	
Ethernet1/0/8	
Ethernet1/0/9	
Ethernet1/0/10	
Ethernet1/0/11	
Ethernet1/0/12	
Ethernet1/0/13	

#### 4.3.1.4 Port combo forced mode config.

Choose **Port configuration > Ethernet port configuration > Port combo forced mode config**, and the following page appears. You can set the combination models to copper-forced, copper-preferred-auto, SFP-forced or SFP-preferred-auto for each port.

Port combo forced mode config	
Port	Ethernet1/0/1 ▾
forced mode	copper-forced ▾
<input type="button" value="Apply"/>	

Information feedback window	
Port	forced mode
Ethernet1/0/1	no support
Ethernet1/0/2	no support
Ethernet1/0/3	no support
Ethernet1/0/4	no support
Ethernet1/0/5	no support
Ethernet1/0/6	no support
Ethernet1/0/7	no support
Ethernet1/0/8	no support
Ethernet1/0/9	no support
Ethernet1/0/10	no support
Ethernet1/0/11	no support

---

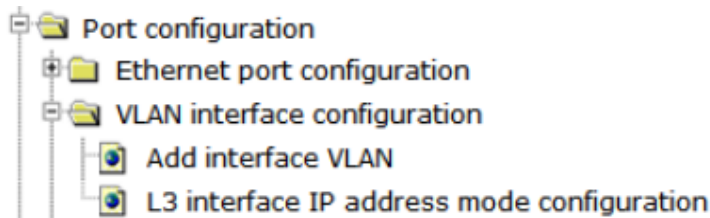
#### 4.3.1.5 Port scan mode.

Choose **Port configuration > Ethernet port configuration > Port scan mode**, and the following page appears. You can change the port scan mode to Mode-interrupt or Mode-poll mode.

port scan mode	
port scan mode	Mode-interrupt ▼
<div>Apply</div>	

#### 4.3.2 VLAN interface configuration.

Choose **Port configuration > VLAN interface configuration**, and the following page appears. There are "Add interface VALN", "L3 interface IP address mode configuration", configuration web pages.



##### 4.3.2.1 Add interface configuration.

Choose **Port configuration > VLAN interface configuration > Add interface configuration**, and the following page appears. You can add or remove a VLAN interface.

Add interface VLAN	
VLAN ID	1 ▼
Operation	Add ▼
<div>Apply</div>	

Vlan ID	State
Vlan1	Layer 3 interface

##### 4.3.2.2 L3 interface IP address mode configuration.

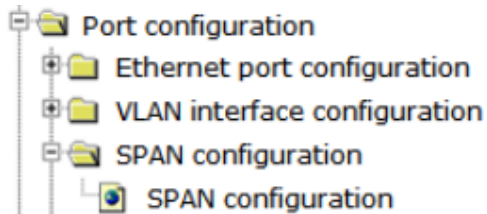
Choose **Port configuration > VLAN interface configuration > L3 interface IP address mode configuration**, and the following page appears. Here you can add or remove the L3 interface mode, set IP mode, the interface IP address, interface network mask.

L3 interface IP address mode configuration	
VLAN interface	Vlan1
IP mode	Specify IP address
Interface IP address	
Interface network mask	
Operation	Add
Apply	

VLAN interface	IP mode	Interface IP address	Interface network mask
Vlan1	Specify IP address	192.168.2.1	255.255.255.0

### 4.3.3 SPAN configuration.

Choose **Port configuration > SPAN configuration**, and the following page appears.



#### 4.3.3.1 SPAN configuration.

Choose **Port configuration > SPAN configuration > SPAN configuration**, and the following page appears. You can set the destination and source port parameters, also can set the Remote-SPAN configuration.

Destination port (SPAN) configuration	
Session	1
Destination port (SPAN)	1/0/1
Operation	Add
Apply	

Rspan vlan configuration	
VLAN name	
Operation	Add
Apply	

SPAN configuration	
Session	Destination port (SPAN)

relector port (SPAN) configuration	
Session	1
Port	Ethernet1/0/1
Operation	Add
Apply	

Source port (SPAN) configuration	
Session	1
Source port (SPAN) list	
CPU to be used for source port	
Access list	
Mirror direction	both
Operation	Add
Apply	

remote vlan configuration	
Session	1
VLAN name	
Operation	Add
Apply	

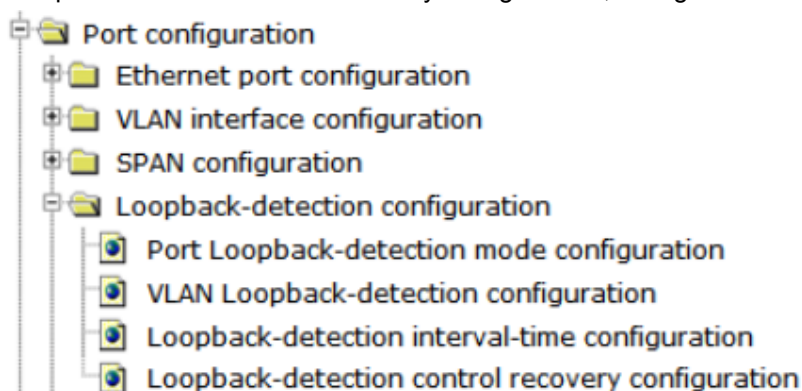
Source port (SPAN) list							
session 1		session 2		session 3		session 4	
Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx



---

### 4.3.4 Loopback-detection configuration.

Choose **Port configuration > Loopback-detection configuration**, and the following page appears. There are "Port Loopback-detection mode configuration", "VLAN Loopback-detection configuration", "Loopback-detection interval-time configuration", "Loopback-detection control recovery configuration", configuration web pages.



#### 4.3.4.1 Port Loopback-detection mode configuration.

Choose **Port configuration > Loopback-detection configuration > Port Loopback-detection mode configuration**, and the following page appears. You can change the Loopback-detection mode to shutdown or block for each port.

Port Loopback-detection mode configuration	
Port	Ethernet1/0/1 ▾
Loopback-detection mode	shutdown ▾
Operation	Add ▾
<div>Apply</div>	

Information feedback window	
Port	Loopback-detection mode
Ethernet1/0/1	no control mode
Ethernet1/0/2	no control mode
Ethernet1/0/3	no control mode
Ethernet1/0/4	no control mode
Ethernet1/0/5	no control mode
Ethernet1/0/6	no control mode
Ethernet1/0/7	no control mode
Ethernet1/0/8	no control mode
Ethernet1/0/9	no control mode
Ethernet1/0/10	no control mode
Ethernet1/0/11	no control mode
Ethernet1/0/12	no control mode
Ethernet1/0/13	no control mode
Ethernet1/0/14	no control mode

---

#### 4.3.4.2 VLAN Loopback-detection configuration.

Choose **Port configuration > Loopback-detection configuration > VLAN Loopback-detection configuration**, and the following page appears. You can specify the VLAN that loop detection on or off.

VLAN Loopback-detection configuration	
Port	Ethernet1/0/1 ▼
VLAN ID	<input type="text"/>
Operation	Add ▼
<input type="text"/>	
<input type="button" value="Apply"/>	

#### 4.3.4.3 Loopback-detection interval-time configuration.

Choose **Port configuration > Loopback-detection configuration > Loopback-detection interval-time configuration**, and the following page appears. You can set no Loopback-detection interval time and Loopback-detection interval time.

Loopback-detection interval-time configuration	
Loopback-detection interval time	<input type="text"/>
no Loopback-detection interval time	<input type="text"/>
Operation	Configuration ▼
<input type="text"/>	
<input type="button" value="Apply"/>	

Information feedback window	
Loopback-detection interval time	no Loopback-detection interval time
5	3

#### 4.3.4.4 Loopback-detection control recovery configuration.

Choose **Port configuration > Loopback-detection configuration > Loopback-detection control recovery configuration**, and the following page appears. You can set the recovery detection interval to allow switch recovery the connection automatically after remove the loop cable.

Loopback-detection control recovery configuration	
Recovery switch timeout	<input type="text"/>
<input type="text"/>	
<input type="button" value="Apply"/>	

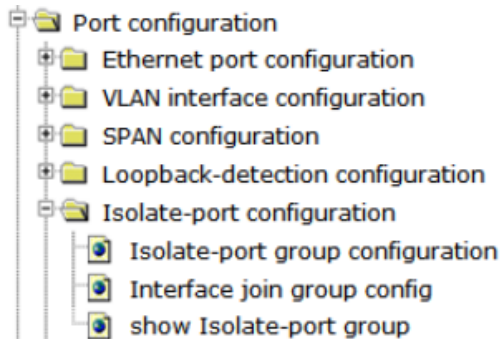
Information feedback window
-----------------------------

---

### 4.3.5 Isolate-port configuration.

Choose **Port configuration > Isolate-port configuration**, and the following page appears.

There are "Isolate-port configuration", "Interface join group config", "show Isolate-port group", configuration web pages.



#### 4.3.5.1 Isolate-port configuration.

Choose **Port configuration > Isolate-port configuration > Isolate-port configuration**, and the following page appears. You can add or remove an Isolate-port group.

Isolate-port group configuration	
Group name	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.3.5.2 Interface join group config.

Choose **Port configuration > Isolate-port configuration > Interface join group config**, and the following page appears. You can add or remove a port to an isolation group.

Interface join group config	
Group name	<input type="text"/>
Port	Ethernet1/0/1 ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.3.5.3 Show Isolate-port group.

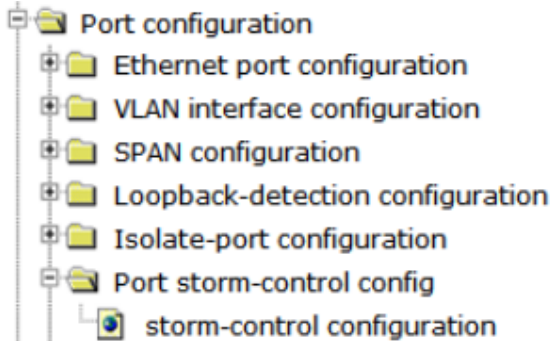
Choose **Port configuration > Isolate-port configuration > show Isolate-port group**, and the following page appears. You can show the group number for each group. Space means show all groups.

---

show Isolate-port group	
Group name	<input type="text"/>
<input type="button" value="Apply"/>	

#### 4.3.6 Port storm-control config

Choose **Port configuration > Port storm-control config**, and the following page appears.



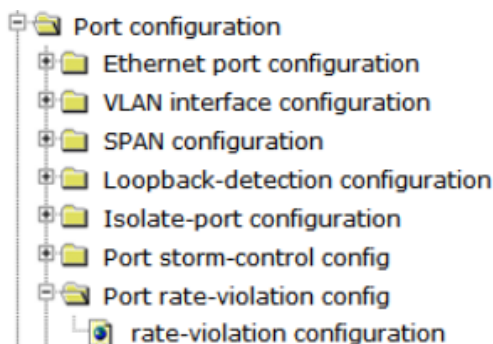
##### 4.3.6.1 Storm-control config

Choose **Port configuration > Port storm-control config > Storm-control configuration**, and the following page appears. You can choose the port for the configure storm-control rule. The storm-control detect type include broadcast, multicast and unicast frame, and the measure unit could be kbps or pps, the threshold value rang is 1-1000000.

storm-control configuration	
Port	Ethernet1/0/1 ▼
storm-control type	broadcast ▼
storm-control measure	kbps ▼
storm-control value	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.3.7 Port rate-violation config

Choose **Port configuration > Port rate-violation config**, and the following page appears.



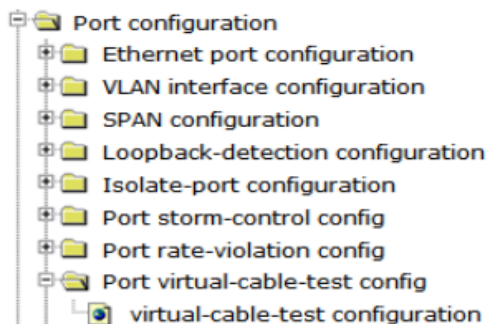
#### 4.3.7.1 Port rate-violation config

Choose **Port configuration > Port rate-violation config > Rate-violation configuration**, and the following page appears. You can choose the port for the rate-violation rule, the detecting data type include all, broadcast, control, multicast and unicast, the rate-violation value range is 200-2000000, the control mode include shutdown, shutdown recovery and block, and the recover time range is 0-86400.

Port rate-violation config	
Port	Ethernet1/0/1
rate-violation type	all
rate-violation value	
rate-violation control mode	shutdown
rate-violation recover time	
Operation	Add
<input type="button" value="Apply"/>	

#### 4.3.8 Port virtual-cable-test config.

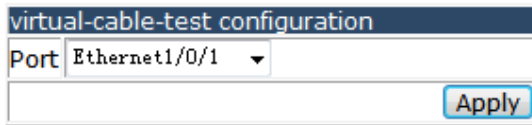
Choose **Port configuration > Port virtual-cable-test config**, and the following page appears.



---

#### 4.3.8.1 Virtual-cable-test configuration.

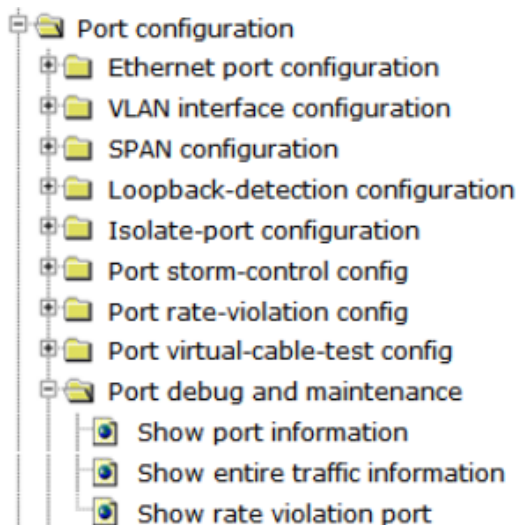
Choose **Port configuration > Port virtual-cable-test config > Virtual-cable-test configuration**, and the following page appears. You can check the connected status for each port.



virtual-cable-test configuration	
Port	Ethernet1/0/1 ▼
<div>Apply</div>	

#### 4.3.9 Port debug and maintenance.

Choose **Port configuration > Port debug and maintenance**, and the following page appears. There are "Show port information", "Show entire traffic information", "Show rate violation port", configuration web pages.



##### 4.3.9.1 Show port information.

Choose **Port configuration > Port debug and maintenance > Show port information**, and the following page appears. You can show the current detail information for each port.

Please select port: Ethernet1/0/1 ▼

#### Information feedback window

##### Interface brief:

Ethernet1/0/1 is down, line protocol is down  
Ethernet1/0/1 is layer 2 port, alias name is (null), index is 1  
Hardware is Gigabit-IX, address is 00-e0-53-16-d0-01  
PVID is 1  
MTU 1500 bytes, BW 10000 Kbit  
Time since last status change: 0w- 0d- 3h- 26m- 58s (12418 seconds)  
Encapsulation ARPA, Loopback not set  
Auto-duplex , Auto-speed  
FlowControl is off, MDI type is auto

##### Transceiver info:

##### Statistics:

5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
The last 5 second input rate 0 bits/sec, 0 packets/sec  
The last 5 second output rate 0 bits/sec, 0 packets/sec  
Input packets statistics:  
0 input packets, 0 bytes, 0 no buffer  
0 unicast packets, 0 multicast packets, 0 broadcast packets  
0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,  
0 abort, 0 length error, 0 undersize 0 jabber, 0 fragments , 0 pause frame  
Output packets statistics:  
0 output packets, 0 bytes, 0 underruns  
0 unicast packets, 0 multicast packets, 0 broadcast packets  
0 output errors, 0 collisions, 0 late collisions , 0 pause frame  
Input and output packets by length:  
(64) bytes: 0, (65-127) bytes: 0,  
(128-255) bytes: 0, (256-511) bytes: 0,  
(512-1023) bytes: 0, (1024-1518) bytes: 0

### 4.3.9.2 Show entire traffic information.

Choose **Port configuration > Port debug and maintenance > Show entire traffic information**, and the following page appears. You can show the statistics data for the receiving and transmission packets for all ports.

Show entire traffic information							
Port	Receiving statistics						Error packets
	Total packets	Error packets	Dropped packets	5 minute rate(packets/sec)	Last 5 second rate(packets/sec)	Total packets	
Ethernet1/0/1	0	0	0	0	0	0	0
Ethernet1/0/2	0	0	0	0	0	0	0
Ethernet1/0/3	0	0	0	0	0	0	0
Ethernet1/0/4	0	0	0	0	0	0	0
Ethernet1/0/5	0	0	0	0	0	0	0
Ethernet1/0/6	0	0	0	0	0	0	0
Ethernet1/0/7	45438	0	0	3	0	57371	0
Ethernet1/0/8	0	0	0	0	0	0	0
Ethernet1/0/9	0	0	0	0	0	0	0
Ethernet1/0/10	0	0	0	0	0	0	0
Ethernet1/0/11	0	0	0	0	0	0	0
Ethernet1/0/12	0	0	0	0	0	0	0
Ethernet1/0/13	0	0	0	0	0	0	0
Ethernet1/0/14	0	0	0	0	0	0	0
Ethernet1/0/15	0	0	0	0	0	0	0
Ethernet1/0/16	0	0	0	0	0	0	0
Ethernet1/0/17	0	0	0	0	0	0	0
Ethernet1/0/18	0	0	0	0	0	0	0
Ethernet1/0/19	0	0	0	0	0	0	0
Ethernet1/0/20	0	0	0	0	0	0	0
Ethernet1/0/21	0	0	0	0	0	0	0

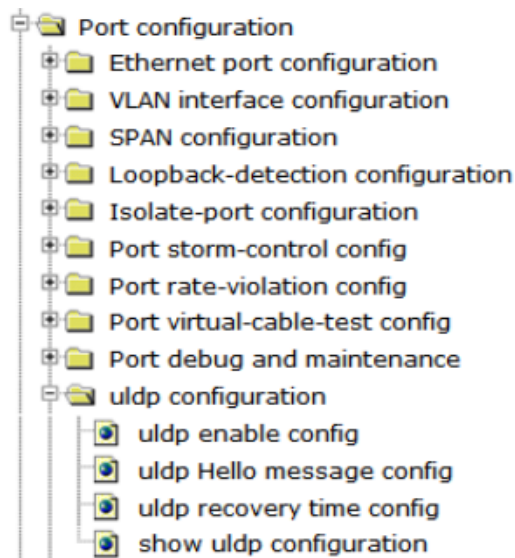
### 4.3.9.3 Show rate violation port.

Choose **Port configuration > Port debug and maintenance > Show rate violation port**, and the following page appears. Here you can show the port rate violation state information.

Rate-violation port state information		
Port	Port rate-violation control mode	Rate-violation port state

### 4.3.10 ULDP configuration.

Choose **Port configuration > ULDP configuration**, and the following page appears. There are "ULDP enable config", "ULDP Hello message", "ULDP recovery time config", "Show ULDP configuration", configuration web pages.



#### 4.3.10.1 ULDP enable config.

Choose **Port configuration > ULDP configuration > ULDP enable config**, and the following page appears. You can set the ULDP configuration for the global device or for every independent port. For global the type include ULDP enable, ULDP aggressive-mode, ULDP manual shutdown and ULDP reset all port. And for one port the type include ULDP port enable, ULDP port aggressive-mode, ULDP reset port.

uldp global enable configuration	
uldp global enable type	uldp enable
Operation	Enable
Apply	

uldp port enable configuration	
Port	Ethernet1/0/1
uldp port enable type	uldp port enable
Operation	Enable
Apply	



---

#### 4.3.10.2 ULDP Hello message config.

Choose **Port configuration > ULDP configuration > ULDP Hello message config**, and the following page appears. You can set the Hello message interval.

uldp Hello message config	
uldp Hello message time	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

#### 4.3.10.3 ULDP recovery time config.

Choose **Port configuration > ULDP configuration > ULDP recovery time config**, and the following page appears. Here you can set the recovery interval.

uldp recovery time config	
uldp Hello message time	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

#### 4.3.10.3 Show ULDP configuration.

Choose **Port configuration > ULDP configuration > Show ULDP configuration**, and the following page appears. Here you can show each port configured ULDP.

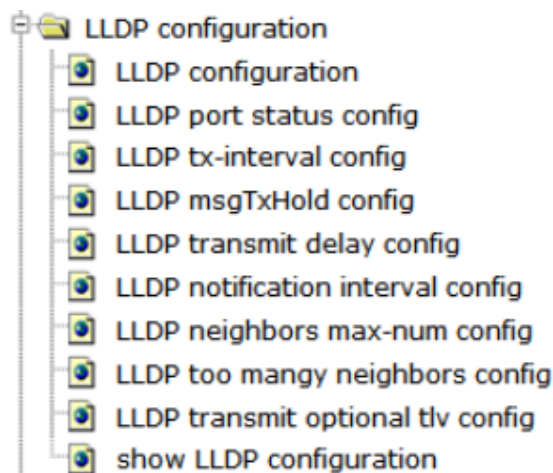
show uldp configuration	
Port	Ethernet1/0/1 ▼
<input type="button" value="Apply"/>	

Information feedback window
switch# show uldp interface Ethernet1/0/1 ULDP has not been enabled global!

#### 4.3.11 LLDP configuration.

Choose **Port configuration > LLDP configuration**, and the following page appears. There are "LLDP configuration", "LLDP port status config", "LLDP tx-interval config", "LLDP msgTxHold config", "LLDP transmit delay config", "LLDP notification

interval config", "LLDP neighbors max-num config", "LLDP too many neighbors config", "LLDP transmit optional tlv config", "show LLDP configuration", configuration web pages.



#### 4.3.11.1 LLDP configuration.

Choose **Port configuration > LLDP configuration > LLDP configuration**, and the following page appears. You can enable the LLDP configuration for the global device or for every independent port. For one port the enable type include LLDP port enable and LLDP port trap enable.

LLDP global enable configuration	
lldp enable	Enable ▼
<input type="button" value="Apply"/>	

LLDP port enable configuration	
Port	Ethernet1/0/1 ▼
LLDP port enable type	LLDP port enable ▼
Operation	Enable ▼
<input type="button" value="Apply"/>	

#### 4.3.11.2 LLDP port status config.

Choose **Port configuration > LLDP configuration > LLDP port status configuration**, and the following page appears. You can set the LLDP status for each port, and the options include send, receive, both and disable.

---

LLDP port status config	
Port	Ethernet1/0/1 ▼
LLDP port status	send ▼
<div>Apply</div>	

#### 4.3.11.3 LLDP tx-interval config.

Choose **Port configuration > LLDP configuration > LLDP tx-interval config**, and the following page appears. You can set the interval time that device sending LLDP Hello message.

LLDP tx-interval config	
lldp Hello message time	<input type="text"/>
Operation	Configuration ▼
<div>Apply</div>	

#### 4.3.11.4 LLDP msgTxHold config.

Choose **Port configuration > LLDP configuration > LLDP msgTxHold config**, and the following page appears. You can set the LLDP aging time algorithm.

LLDP msgTxHold config	
LLDP msgTxHold value	<input type="text"/>
Operation	Configuration ▼
<div>Apply</div>	

#### 4.3.11.5 LLDP transmit delay config.

Choose **Port configuration > LLDP configuration > LLDP transmit delay config**, and the following page appears. You can modify the LLDP packets propagation delay values.

LLDP transmit delay config	
LLDP transmit delay value	<input type="text"/>
Operation	Configuration ▼
<div>Apply</div>	

#### 4.3.11.6 LLDP notification interval config.

Choose **Port configuration > LLDP configuration > LLDP notification interval config**, and the following page appears. You can set the LLDP notification interval configurations.

---

LLDP notification interval config	
LLDP notification interval value	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.3.11.7 LLDP neighbors max-num config.

Choose **Port configuration > LLDP configuration > LLDP neighbors max-num config**, and the following page appears. You can set the amount of message number in the Remote MIB Table.

LLDP neighbors max-num config	
Port	Ethernet1/0/1 ▾
LLDP neighbors max-num value	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.3.11.8 LLDP too mangy neighbors config.

Choose **Port configuration > LLDP configuration > LLDP too mangy neighbors config**, and the following page appears. You can choose to discard or delete message after fill full of the Remote table.

LLDP too mangy neighbors config	
Port	Ethernet1/0/1 ▾
LLDP too mangy neighbors value	discard ▾
<input type="button" value="Apply"/>	

#### 4.3.11.9 LLDP transmit optional tlv config.

Choose **Port configuration > LLDP configuration > LLDP transmit optional tlv config**, and the following page appears. You can choose the optional tlv for the transmitting LLDP message.

LLDP transmit optional tlv config	
Port	Ethernet1/0/1 ▾
LLDP Port description	<input type="checkbox"/>
LLDP System capability	<input type="checkbox"/>
LLDP System description	<input type="checkbox"/>
LLDP System name	<input type="checkbox"/>
<input type="button" value="Apply"/>	

#### 4.3.11.10 show LLDP configuration.

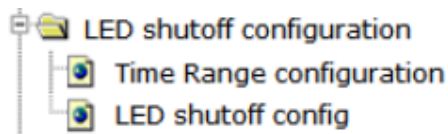
Choose **Port configuration > LLDP configuration > show LLDP configuration**, and the following page appears. You can show the status and statistics data for LLDP function.

show LLDP configuration	
LLDP too many neighbors value	show LLDP
Port	all
<input type="button" value="Apply"/>	

#### 4.3.12 LED shutoff configuration.

Choose **Port configuration > LED shutoff configuration**, and the following page appears.

There are "Time Range configuration", "LED shutoff config", configuration web pages.



##### 4.3.12.1 Time Range configuration.

Choose **Port configuration > LED shutoff configuration > Time Range configuration**, and the following page appears. You can set the time range for the LED shutoff rule.

In the absolute mode you must input the start-time, end-time is not necessary. You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic. You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values, separate them with ",", such as: 1-7:monday-sunday; 127:daily; 31:weekdays; 96:weekend. Input date format: YYYY.MM.DD. Input week format: number (1:Monday etc.), if input multi-week values, separate them with ",", such as: 1,2 identify monday&tuesday.. Input time format: HH:MM:SS.

Time range configuration	
Time range name	<input type="text"/>
Time range type	absolute <input type="checkbox"/>
Start Time	<input type="text"/>
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
End Time	<input type="text"/>
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
Operation type	Add <input type="button" value="Apply"/>

---

#### 4.3.12.2 LED shutoff config.

Choose **Port configuration > LED shutoff configuration > LED shutoff config**, and the following page appears. You can design the LED to open or close at the time you configured.

LED shutoff configuration	
Time range name	<input type="text"/>
LED state	Open <input type="button" value="v"/>
Operation	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

#### 4.3.13 Jumbo packet forwarding configuration.

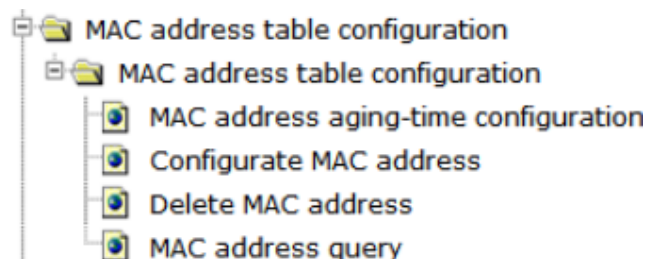
Choose **Port configuration > Jumbo packet forwarding configuration**, and the following page appears. You can set the size of the Jumbo packet ranging 1500-16000.

Jumbo packet forwarding configuration	
Jumbo packet size	<input type="text"/>
Operation	Configuration <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Information feedback window	
Jumbo packet forwarding configuration	Jumbo packet size
Disable	1500

### 4.4 MAC address table configuration.

Choose **MAC address table configuration > MAC address table configuration**, and the following page appears. There are "MAC address aging-time configuration", "Configure MAC address", "Delete MAC address", "MAC address query", configuration web pages.



## 4.4.1 MAC address table configuration.

Choose **MAC address table configuration > MAC address table configuration > MAC address aging-time configuration**, and the following page appears. You can set the MAC address aging time.

MAC address aging-time configuration	
MAC address aging-time	
Operation	Configuration ▾
<input type="button" value="Apply"/>	

MAC address aging-time
300

## 4.4.2 Configuration MAC address.

Choose **MAC address table configuration > MAC address table configuration > Configuration MAC address**, and the following page appears. You can set a static MAC address corresponding to a physic port. Also you can block the data with a static MAC address as its source or destination address.

Configure static MAC address	
MAC address	
VLAN ID	1 ▾
Port list	Ethernet1/0/1 ▾
Operation	Add ▾
<input type="button" value="Apply"/>	

Configure blackhole MAC address	
MAC address	
VLAN ID	1 ▾
Blackhole based type	▾
Operation	Add ▾
<input type="button" value="Apply"/>	

MAC address	VLAN ID	Port
-------------	---------	------

## 4.4.3 Delete MAC address.

Choose **MAC address table configuration > MAC address table configuration > Delete MAC address**, and the following page appears. You can delete MAC address from the static MAC address table, dynamic MAC address table or blackhole table by VLAN ID, MAC or port.

Delete MAC address	
Port status	Static ▾
Delete by VLAN ID	1 ▾ <input type="checkbox"/> Select
Delete by MAC	<input type="text"/> <input type="checkbox"/> Select
Delete by port	Ethernet1/0/1 ▾ <input type="checkbox"/> Select
<input type="button" value="Delete"/>	

MAC address	VLAN ID	Status
-------------	---------	--------

---

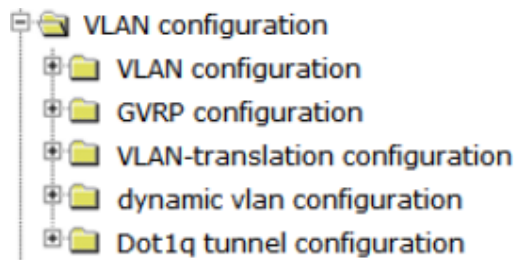
#### 4.4.4 MAC address query.

Choose **MAC address table configuration > MAC address table configuration > MAC address query**, and the following page appears. You can show the static MAC address table, dynamic MAC address table or blackhole table by VLAN ID, MAC or port.

MAC address query		
Port status	Static ▾	<input type="checkbox"/> Select
Query by MAC	<input type="text"/>	<input type="checkbox"/> Select
Query by VLAN ID	1 ▾	<input type="checkbox"/> Select
Query by port	Ethernet1/0/1 ▾	<input type="checkbox"/> Select
		<input type="button" value="Apply"/>

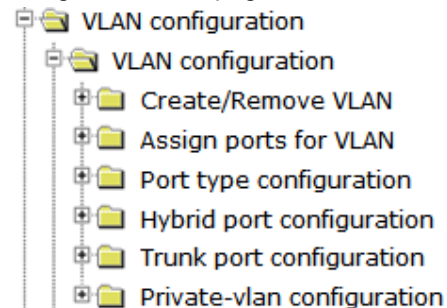
#### 4.5 VLAN configuration.

Choose **VLAN configuration**, and the following page appears. There are "VLAN configuration", "GVRP configuration", "VLAN-translation configuration", "Dynamic VLAN configuration", "Dot1q tunnel configuration", configuration web pages.



##### 4.5.1 VLAN configuration.

Choose **VLAN configuration > VLAN configuration**, and the following page appears. There are "Create/Remove", "Assign ports for VLAN", "Port type configuration", "Hybrid port configuration", "Trunk port configuration", "Private-vlan configuration", configuration web pages.





#### 4.5.1.1 VLAN ID configuration.

Choose **VLAN configuration > VLAN configuration > Create/Remove VLAN > VLAN ID configuration**, and the following page appears. Here you are allowed to create or delete VLAN. VLAN type is divided into Private VLAN (isolated), Private VLAN (community), Private VLAN (primary) and universal VLAN.

VLAN ID configuration	
VLAN ID	<input type="text"/>
VLAN Name	<input type="text"/>
VLAN Type	<input type="text"/>
Operation	<input type="text" value="Add"/>
<input type="button" value="Apply"/>	

VLAN ID information		
VLAN ID	VLAN Name	VLAN Type
1	default	universal vlan

#### 4.5.1.2 Assign ports for VLAN.

Choose **VLAN configuration > VLAN configuration > Assign ports for VLAN > Assign ports for VLAN**, and the following page appears. You can appoint a port to a configured VLAN.

Assign ports for VLAN	
VLAN ID	<input type="text" value="1"/>
Port	<input type="text" value="Ethernet1/0/1"/>
Operation	<input type="text" value="Add"/>
<input type="button" value="Apply"/>	

Information feedback window				
Universal vlan:				
VLAN Name	Type	Media	Ports	
1	default	Static	ENET	Ethernet1/0/1 Ethernet1/0/2 Ethernet1/0/3 Ethernet1/0/4 Ethernet1/0/5 Ethernet1/0/6 Ethernet1/0/7 Ethernet1/0/8 Ethernet1/0/9 Ethernet1/0/10 Ethernet1/0/11 Ethernet1/0/12 Ethernet1/0/13 Ethernet1/0/14 Ethernet1/0/15 Ethernet1/0/16 Ethernet1/0/17 Ethernet1/0/18 Ethernet1/0/19 Ethernet1/0/20 Ethernet1/0/21 Ethernet1/0/22 Ethernet1/0/23 Ethernet1/0/24 Ethernet1/0/25 Ethernet1/0/26 Ethernet1/0/27 Ethernet1/0/28
Private vlan:				
VLAN Name	Type	Asso VLAN	Ports	

#### 4.5.1.3 Set port mode(access/hybrid/trunk).

Choose **VLAN configuration > VLAN configuration > Port type configuration > Set port mode(access/hybrid/trunk)**, and the following page appears. You can change any port to access, trunk or hybrid mode. Also you can choose enable VLAN ingress check or disable VLAN ingress check mode.

Port mode configuration	
Port	Ethernet1/0/1
Type	access
State	Enable VLAN ingress check
<input type="button" value="Apply"/>	

Port mode configuration		
Port	Type	State
Ethernet1/0/1	access	Open
Ethernet1/0/2	access	Open
Ethernet1/0/3	access	Open
Ethernet1/0/4	access	Open
Ethernet1/0/5	access	Open
Ethernet1/0/6	access	Open
Ethernet1/0/7	access	Open
Ethernet1/0/8	access	Open
Ethernet1/0/9	access	Open
Ethernet1/0/10	access	Open

#### 4.5.1.4 VLAN setting for hybrid port.

Choose **VLAN configuration > VLAN configuration > Hybrid port configuration > VLAN setting for hybrid port**, and the following page appears. You can set Hybrid native VLAN ID for the hybrid port as its PVID. Also You can design which VLAN can be allowed to access to the hybrid port and whether tag or Untag the data, and the operation method including Add all, Add, Except add, Cover add and remove.

Set hybrid native VLAN	
Port	
Hybrid native VLAN	
Operation	Add
<input type="button" value="Apply"/>	

Set hybrid allow VLAN	
Port	
Hybrid allowed VLAN list	
Operation	Add all
Tagged	Untag
<input type="button" value="Apply"/>	

Port	Hybrid native VLAN	Hybrid Tagged allowed VLAN list	Hybrid UnTagged allowed VLAN list
------	--------------------	---------------------------------	-----------------------------------

---

#### 4.5.1.5 VLAN setting for trunk port.

Choose **VLAN configuration > Trunk port configuration > VLAN setting for trunk port**, and the following page appears. You can set Trunk native VLAN ID for the trunk port as its PVID. Also You can design which VLAN can be allowed to access to the trunk port, the operation method including Add all, Add, Except add, Cover add and remove.

Set trunk native VLAN	
Port	<input type="text"/>
Trunk native VLAN	<input type="text"/>
Operation	<input type="text" value="Add"/>
<input type="button" value="Apply"/>	

Set trunk allow VLAN	
Port	<input type="text"/>
Trunk allowed VLAN list	<input type="text"/>
Operation	<input type="text" value="Add all"/>
<input type="button" value="Apply"/>	

Port Trunk native VLAN Trunk allowed VLAN list

#### 4.5.1.6 Private-vlan association.

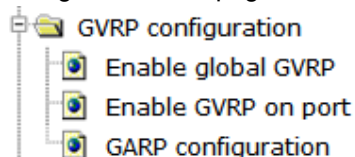
Choose **VLAN configuration > Private-vlan configuration > Private-vlan association**, and the following page appears. You can set the association VLAN to bind with the primary-vlan, then the members in association VLANs can communicate with primary-vlan.

Private-vlan association	
Designate Primary-vlan	<input type="text"/>
Association VLAN list	<input type="text"/>
Operation	<input type="text" value="Configuration"/>
<input type="button" value="Apply"/>	

Primary-vlan Association VLAN list

#### 4.5.2 GVRP configuration.

Choose **VLAN configuration > GVRP configuration**, and the following page appears. There are "Enable global GVRP", "Enable GVRP on port", "GARP configuration", configuration web pages.



---

#### 4.5.2.1 Enable global GVRP.

Choose **VLAN configuration > GVRP configuration > Enable global GVRP**, and the following page appears. You can enable or disable the global GVRP. To configure port GVRP must enable the global GVRP first.

Enable global GVRP	
Enable/Disable global GVRP	Enable ▾
<div>Apply</div>	

Enable global GVRP	
GVRP status	Enable

#### 4.5.2.2 Enable GVRP on port.

Choose **VLAN configuration > GVRP configuration > Enable GVRP on port**, and the following page appears. You can enable or disable GVRP function for each port.

Enable GVRP on port	
Port	▾
Enable/Disable GVRP	Enable ▾
<div>Apply</div>	

Port	GVRP Status
------	-------------

#### 4.5.2.3 GARP configuration.

Choose **VLAN configuration > GVRP configuration > GARP configuration**, and the following page appears. You can set the GVRP timer parameters.

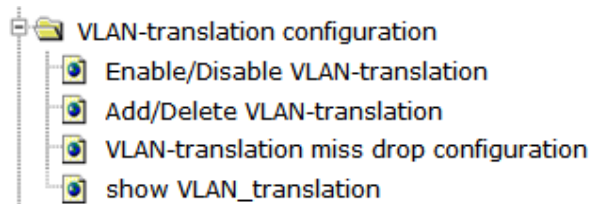
GARP parameters configuration	
Join timer	200
Leave timer	600
Leaveall timer	10000
Operation	Configuration ▾
<div>Apply</div>	

#### 4.5.3 VLAN-translation configuration.

Choose **VLAN configuration > VLAN-translation configuration**, and the following page appears.

---

There are "Enable/Disable VLAN-translation", "Add/Delete VLAN-translation", "VLAN-translation miss drop configuration", "show VLAN-translation", configuration web pages.



#### 4.5.3.1 Enable/Disable VLAN-translation.

Choose **VLAN configuration > VLAN-translation configuration > Enable/Disable VLAN-translation**, and the following page appears. You can enable or disable the port VLAN translation mode.

Enable/Disable VLAN-translation	
Port	Ethernet1/0/1
Enable/Disable VLAN-translation	Enable
<input type="button" value="Apply"/>	

Port	VLAN-translation Status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable
Ethernet1/0/10	Disable
Ethernet1/0/11	Disable
Ethernet1/0/12	Disable
Ethernet1/0/13	Disable

#### 4.5.3.2 Add/Delete VLAN-translation.

Choose **VLAN configuration > VLAN-translation configuration > Add/Delete VLAN-translation**, and the following page appears. You can set the translation policy for each port, data transmit in or out the port the source VLAN ID will be translated to the destination VLAN ID.

Add/Delete VLAN-translation	
Port	Ethernet1/0/1 ▼
source vlan ID	Vlan1 ▼
destination vlan ID	Vlan1 ▼
dirction	in ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.5.3.3 VLAN-translation miss drop configuration.

Choose **VLAN configuration > VLAN-translation configuration > VLAN-translation miss drop configuration**, and the following page appears. You can decide to whether discard data failed to execute VLAN-translation and the transmission direction for the operation.

VLAN-translation miss drop configuration	
Port	Ethernet1/0/1 ▼
dirction	both ▼
Operation	Configuration ▼
<input type="button" value="Apply"/>	

#### 4.5.3.4 Show VLAN-translation.

Choose **VLAN configuration > VLAN-translation configuration > Show VLAN-translation**, and the following page appears. You can show the VLAN-translation information for all ports enabled this function.

show VLAN_translation	
<input type="button" value="Apply"/>	

Information feedback window
switch# show vlan-translation

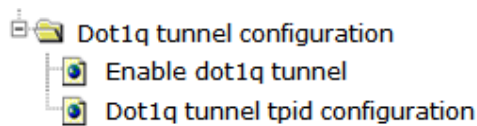
#### 4.5.4 Dynamic VLAN configuration.

Choose **VLAN configuration > Dynamic VLAN configuration > Protocol VLAN configuration > Protocol VLAN mode configuration**, and the following page appears. You can set protocol-vlan rules, the protocol mode include Ethernet II, snap, LLC and all, the protocol mode ID rang for ethernet II or snap rang is 1-65536, for llc is 0-255, the SSAP ID just for llc rang is 0-255, the priority ID rang is 0-7.

protocol vlan mode configuration	
VLAN interface	Vlan1 ▾
protocol mode	ethernetII ▾
protocol mode ID	<input type="text"/>
SSAP ID	<input type="text"/>
priority ID	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.5.5 Dot1q tunnel configuration.

Choose **VLAN configuration > Dot1q tunnel configuration**, and the following page appears. There are "Enable dot1q tunnel", "Dot1q tunnel tpid configuration", configuration web pages.



##### 4.5.5.1 Enable dot1q tunnel.

Choose **VLAN configuration > Dot1q tunnel configuration > Enable dot1q tunnel**, and the following page appears. You can enable or disable dot1q tunnel function for every Trunk port.

Enable dot1q tunnel	
Port	Ethernet1/0/1 ▾
Operation	Enable ▾
<input type="button" value="Apply"/>	

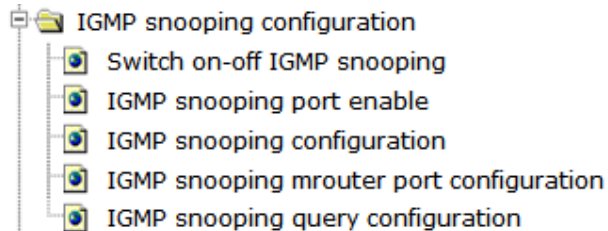
##### 4.5.5.2 Dot1q tunnel tpid configuration.

Choose **VLAN configuration > Dot1q tunnel configuration > Dot1q tunnel tpid configuration**, and the following page appears. You can configure the Dot1q protocol for trunk, please keep this value the same with the connected device.

Dot1q tunnel tpid configuration	
Port	Ethernet1/0/1 ▼
protocol	0x8100 ▼
protocol ID	<input type="text"/>
<input type="button" value="Apply"/>	

## 4.6 IGMP snooping configuration.

Choose **IGMP snooping configuration**, and the following page appears. There are "Switch on-off IGMP snooping", "IGMP snooping port enable", "IGMP snooping configuration", "IGMP snooping mrouter port configuration", "IGMP snooping query configuration", configuration web pages.



### 4.6.1 Switch on-off IGMP snooping.

Choose **IGMP snooping configuration > Switch on-off IGMP snooping**, and the following page appears. You can open or close the IGMP snooping function.

Switch on-off IGMP snooping	
Switch on-off IGMP snooping	Open ▼
<input type="button" value="Apply"/>	

Switch on-off IGMP snooping	
Switch on-off IGMP snooping	Open

### 4.6.2 IGMP snooping port enable.

Choose **IGMP snooping configuration > IGMP snooping port enable**, and the following page appears. You can open or close the IGMP Snooping function for different VLAN.



IGMP Snooping VLAN config	
VLAN ID	vlan 1 ▼
Operation type	Open ▼
<input type="button" value="Apply"/>	

IGMP Snooping VLAN config	
VLAN ID	Operation type
1	CLOSE

### 4.6.3 IGMP snooping configuration.

Choose **IGMP snooping configuration > IGMP snooping configuration**, and the following page appears. You can set the IGMP Snooping parameters for each VLAN, choose enable Immediate leave configuration and L2-general-querier configuration or not. The default value for Group number is 50 and for Source table number is 40, it is recommended not to change them.

Igmp Snooping Configuration	
VLAN ID	vlan 1 ▼
Immediate leave configuration	immediate leave ▼ <input type="checkbox"/>
L2-general-querier configuration	L2-general-querier ▼ <input type="checkbox"/>
Group number	<input type="text"/> <input type="checkbox"/>
Source table number	<input type="text"/> <input type="checkbox"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

VLAN ID	Immediate leave configuration	L2-general-querier configuration	Group number	Source table number
1	Disable	Disable		

### 4.6.4 IGMP snooping mrouter port configuration.

Choose **IGMP snooping configuration > IGMP snooping mrouter port configuration**, and the following page appears. You can choose the Mrouter port which connecting with the router for VLAN, and the Mrouter port alive time for dynamic Mrouter port.

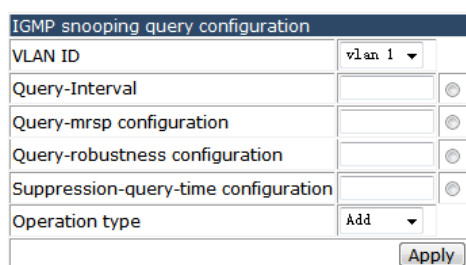
IGMP snooping mrouter port configuration	
VLAN ID	vlan 1 ▼
Mrouter port	Ethernet1/0/1 ▼ <input type="checkbox"/>
MRouter port alive time	<input type="text"/> <input type="checkbox"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

VLAN ID	Mrouter port	MRouter port alive time
1		

---

### 4.6.5 IGMP snooping query configuration.

Choose **IGMP snooping configuration > IGMP snooping query configuration**, and the following page appears. You can set the query parameters for VLAN, the default value for those four options are 125, 10, 2, 255, they are recommended to keep default.



IGMP snooping query configuration

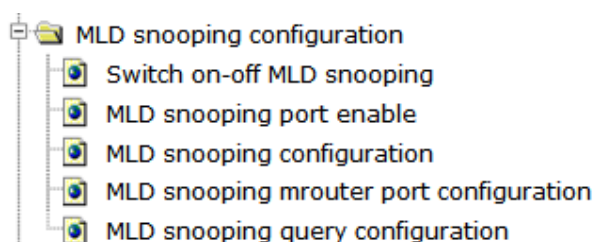
VLAN ID	vlan 1	
Query-Interval		
Query-mrsp configuration		
Query-robustness configuration		
Suppression-query-time configuration		
Operation type	Add	

Apply

VLAN ID	Query-Interval	Query-mrsp configuration	Query-robustness configuration	Suppression-query-time configuration
1				

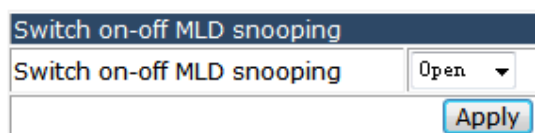
### 4.7 MLD snooping configuration.

Choose **MLD snooping configuration**, and the following page appears. There are "Switch on-off MLD snooping", "MLD snooping port enable", "MLD snooping configuration", "MLD snooping mrouter port configuration", "MLD snooping query configuration", configuration web pages.



#### 4.7.1 Switch on-off MLD snooping.

Choose **MLD snooping configuration > Switch on-off MLD snooping**, and the following page appears. You can open or close the MLD snooping function.



Switch on-off MLD snooping

Switch on-off MLD snooping	Open
----------------------------	------

Apply

---

#### 4.7.2 MLD snooping port enable.

Choose **MLD snooping configuration > MLD snooping port enable**, and the following page appears. You can open or close the MLD snooping function for each VLAN.

MLD Snooping VLAN config	
VLAN ID	vlan 1 ▼
Operation type	Open ▼
<input type="button" value="Apply"/>	

#### 4.7.3 MLD snooping configuration.

Choose **MLD snooping configuration > MLD snooping configuration**, and the following page appears. You can set the MLD Snooping parameters for each VLAN, choose enable Immediate leave configuration and L2-general-querier configuration or not. The default value for Group number is 50 and for Source table number is 40, it is recommended not to change them.

MLD Snooping Configuration		
VLAN ID	vlan 1 ▼	
Immediate leave configuration	immediate leave ▼	<input type="checkbox"/>
L2-general-querier configuration	L2-general-querier ▼	<input type="checkbox"/>
Group number	<input type="text"/>	<input type="checkbox"/>
Source table number	<input type="text"/>	<input type="checkbox"/>
Operation	Configuration ▼	
<input type="button" value="Apply"/>		

#### 4.7.4 MLD snooping mrouter port configuration.

Choose **MLD snooping configuration > MLD snooping mrouter port configuration**, and the following page appears. You can choose the Mrouter port which connecting with the router for VLAN, and the Mrouter port alive time for dynamic Mrouter port.

MLD snooping mrouter port configuration	
VLAN ID	vlan 1 ▼
Mrouter port	Ethernet1/0/1 ▼ <input type="checkbox"/>
MRouter port alive time	<input type="text"/> <input type="checkbox"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

---

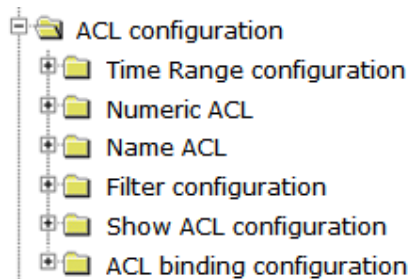
### 4.7.5 MLD snooping query configuration.

Choose **MLD snooping configuration > MLD snooping query configuration**, and the following page appears. You can set the query parameters for VLAN, the default value for those four options are 125, 10, 2, 255, they are recommended to keep default.

MLD snooping query configuration	
VLAN ID	vlan 1 ▼
Query-Interval	<input type="text"/> <input type="radio"/>
Query-mrsp configuration	<input type="text"/> <input type="radio"/>
Query-robustness configuration	<input type="text"/> <input type="radio"/>
Suppression-query-time configuration	<input type="text"/> <input type="radio"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

## 4.8 ACL configuration.

Choose **ACL configuration**, and the following page appears. There are "Time Range configuration", "Numeric ACL", "Name ACL", "Filter configuration", "Show ACL configuration", "ACL binding configuration", configuration web pages.



### 4.8.1 Time Range configuration.

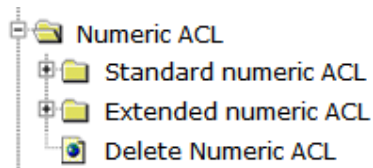
Choose **ACL configuration > Time Range configuration > Time Range configuration**, and the following page appears. You can set the time policies for ACL rules.

In the absolute mode you must input the start-time , end-time is not necessary. You must input the weeks, start-time and end-time, but need not input the date including start and end time in the absolute-periodic. You must input the weeks, start-time and end-time, but need not input the date including start and end time, and may input multi-week values, separate them with ", ", such as: 1-7:monday-sunday; 127:daily; 31:weekdays; 96:weekend. Input date format: YYYY.MM.DD. Input week format: number (1:Monday etc.), if input multi-week values, separate them with ", ", such as: 1,2 identify monday&tuesday.. Input time format: HH:MM:SS.

Time range configuration	
Time range name	<input type="text"/>
Time range type	absolute <input type="checkbox"/>
Start Time	<input type="text"/>
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
End Time	<input type="text"/>
Week	<input type="text"/>
Time	<input type="text"/>
Date	<input type="text"/>
Operation type	Add <input type="button" value="Apply"/>

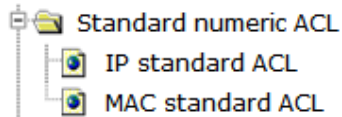
## 4.8.2 Numeric ACL.

Choose **Numeric ACL**, and the following page appears. There are "Standard numeric ACL", "Extended numeric ACL", "Delete Numeric ACL", configuration web pages.



### 4.8.2.1 Standard numeric ACL.

Choose **ACL configuration > Numeric ACL > Standard numeric ACL**, and the following page appears. There are "IP standard ACL", "MAC standard ACL", configuration web pages.



#### 4.8.2.1.1 IP standard ACL.

Choose **ACL configuration > Numeric ACL > Standard numeric ACL > IP standard ACL**, and the following page appears. You can add a ACL rule to permit or deny data from different source address. If the type is Any IP don't need set IP address and mask, if the type is Host IP don't need to set Reverse network mask, if the type is Specified IP the IP address and Reverse network mask decided which IP will be controlled.

IP standard ACL(Number)	
List name	
Rule	permit ▼
Source address type	Any IP ▼
Source IP	
Reverse network mask	
Apply	

Information feedback window  
The count of total acl has been used is 0.

#### 4.8.2.1.2 MAC standard ACL.

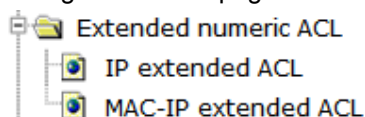
Choose **ACL configuration > Numeric ACL > Standard numeric ACL > MAC standard ACL**, and the following page appears. You can add a MAC ACL rule to permit or deny data from different source MAC address. If the type is Any MAC don't need set MAC address and mask, if the type is Host MAC don't need to set Reverse network mask, if the type is Specified MAC the MAC address and Reverse network mask decided which MAC will be controlled.

MAC standard ACL(Number)	
List name	
Rule	permit ▼
Source address type	Any MAC ▼
Source MAC	
Reverse network mask	
Apply	

Information feedback window  
The count of total acl has been used is 0.

#### 4.8.2.2 Extended numeric ACL.

Choose **ACL configuration > Numeric ACL > Extended numeric ACL**, and the following page appears. There are "IP extended ACL", "MAC-IP extended ACL", configuration web pages.



##### 4.8.2.2.1 IP extended ACL.

Choose **ACL configuration > Numeric ACL > Extended numeric ACL > IP extended ACL**, and the following page appears. You can configure the extended ACL with advanced function include Operation type, Source address, Destination address, IP precedence, TOS, Time range and the protocol features. The Operation type include ICMP, IGMP, TCP, UDP, EIGRP, GRE, IGRP, IPINIP, OSPF, IP, Specified\_protocol.

IP extended ACL(Number)	
Operation type	ICMP
List name	
Rule	permit
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Information feedback window  
The count of total acl has been used is 0.

#### 4.8.2.2.2 MAC-IP extended ACL.

Choose **ACL configuration > Numeric ACL > Extended numeric ACL > MAC-IP extended ACL**, and the following page appears. You can configure the extended MAC-IP ACL with advanced function, and the qualification can be both MAC and IP address.

MAC-IP extended ACL(Number)	
Operation type	ICMP
List name	
Rule	permit
Source address type	Any MAC
Source MAC	
Reverse network mask	
Destination address type	Any MAC
Destination MAC	
Reverse network mask	
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Information feedback window  
The count of total acl has been used is 0.

#### 4.8.2.3Delete Numeric ACL.

Choose **ACL configuration > Numeric ACL > Extended numeric ACL > Delete Numeric ACL**, and the following page appears. You can delete Numeric ACL rules based on their List names.

Delete Numeric ACL

List name

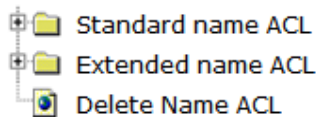
Apply

Information feedback window

The count of total acl has been used is 0.

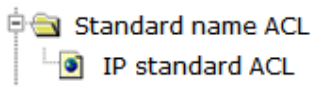
### 4.8.3 Name ACL.

Choose **ACL configuration > Name ACL**, and the following page appears. There are "Standard name ACL", "Extended name ACL", "Delete name ACL", configuration web pages.



#### 4.8.3.1 Standard name ACL.

Choose **ACL configuration > Name ACL > Standard name ACL**, and the following page appears.



##### 4.8.3.1.1 IP standard ACL.

Choose **ACL configuration > Name ACL > Standard name ACL > IP standard ACL**, and the following page appears. You can add a ACL rule to permit or deny data from different source address. The List name must start with letter. If the type is Any IP don't need set IP address and mask, if the type is Host IP don't need to set Reverse network mask, if the type is Specified IP the IP address and Reverse network mask decided which IP will be controlled.

IP standard ACL

List name

Rule

Source address type

Source IP

Reverse network mask

Apply

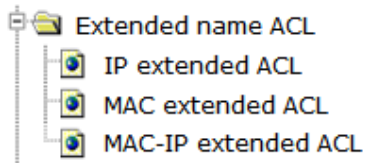
Information feedback window

The count of total acl has been used is 0.

#### 4.8.3.2 Extended name ACL.

Choose **ACL configuration > Name ACL > Extended name ACL**, and the following page appears. There are "IP extended ACL", "MAC extended ACL", "MAC-IP extended ACL", configuration web pages.





#### 4.8.3.2.1 IP extended ACL.

Choose **ACL configuration > Name ACL > Extended name ACL > IP extended ACL**, and the following page appears. You can configure the extended ACL with advanced function include Operation type, Source address, Destination address, IP precedence, TOS, Time range and the protocol features. The List name must start with letter. The Operation type include ICMP, IGMP, TCP, UDP, EIGRP, GRE, IGRP, IPINIP, OSPF, IP, Specified\_protocol.

IP extended ACL	
Operation type	ICMP
List name	
Rule	permit
Source address type	Any IP
Source IP	
Reverse network mask	
Destination address type	Any IP
Destination IP	
Reverse network mask	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
<input type="button" value="Apply"/>	

Information feedback window

The count of total acl has been used is 0.

#### 4.8.3.2.2 MAC extended ACL.

Choose **ACL configuration > Name ACL > Extended name ACL > MAC extended ACL**, and the following page appears. You can configure the extended MAC ACL with advanced function include Source address, Destination address, Packet type, COS, COS mask, VLAN ID, VLAN ID mask, ether Type and ether Type mask. The List name must start with letter. The Packet type include Tagged-802.3, Tagged-eth2, Untagged-802.3, Untagged-eth2.

MAC extended ACL	
List name	
Rule	permit ▼
Source address type	Any MAC ▼
Source MAC	
Reverse network mask	
Destination address type	Any MAC ▼
Destination MAC	
Reverse network mask	
Packet type	none ▼
cos	
cos mask	
VLANID	
VLANID mask	
etherType	
etherType mask	
Apply	

Information feedback window
The count of total acl has been used is 0.

#### 4.8.3.2.3 MAC-IP extended ACL.

Choose **ACL configuration > Name ACL > Extended name ACL > MAC-IP extended ACL**, and the following page appears. You can configure the extended MAC-IP ACL with advanced function, and the qualification can be both MAC and IP address. The List name must start with letter.

MAC-IP extended ACL	
Operation type	ICMP ▼
List name	
Rule	permit ▼
Source address type	Any MAC ▼
Source MAC	
Reverse network mask	
Destination address type	Any MAC ▼
Destination MAC	
Reverse network mask	
Source address type	Any IP ▼
Source IP	
Reverse network mask	
Destination address type	Any IP ▼
Destination IP	
Reverse network mask	
IP precedence	
TOS	
Time range name	
ICMP extended	
ICMP type	
ICMP code	
Apply	

Information feedback window
The count of total acl has been used is 0.

#### 4.8.3.3 Delete Name ACL.

Choose **ACL configuration > Name ACL > Delete name ACL**, and the following page appears. You can delete Name ACL rules based on their List names.

Delete Name ACL	
List name	<input type="text"/>
<input type="button" value="Apply"/>	

Information feedback window
The count of total acl has been used is 0.

#### 4.8.4 Firewall configuration.

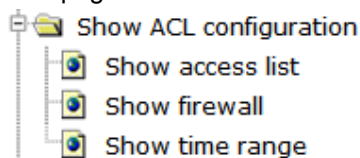
Choose **ACL configuration > Filter configuration > Firewall configuration**, and the following page appears. You must open the Packet filtering function to make the ACL list take effect. The Firewall default action is permit means data mismatching the ACL rule is permitted.

Switch firewall configuration	
Packet filtering	close ▼
Firewall default action	permit ▼
<input type="button" value="Apply"/>	

Switch firewall configuration	
Packet filtering	Firewall default action
CLOSE	permit

#### 4.8.5 Show ACL configuration.

Choose **ACL configuration > Show ACL configuration**, and the following page appears. There are "Show access list", "Show firewall", "Show time range", configuration web pages.



##### 4.8.5.1 Show access list.

Choose **ACL configuration > Show ACL configuration > Show access list**, and the following page appears. You can show the access-list by name or show all table.

Show access list	
Access list	ALL
<input type="button" value="Apply"/>	

Information feedback window
switch# show access-lists
The count of total acl has been used is 0.

---

#### 4.8.5.2 Show firewall.

Choose **ACL configuration > Show ACL configuration > Show firewall**, and the following page appears. You can show the status of firewall.

Show firewall
<div>Refresh</div>

Information feedback window
switch# show firewall Firewall Status: Enable.

#### 4.8.5.3 Show time range.

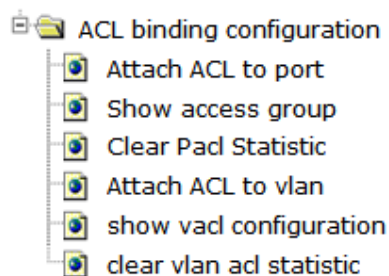
Choose **ACL configuration > Show ACL configuration > Show time range**, and the following page appears. You can show time range list by name or show all table.

Show time range	
Time-range name	ALL
<div>Apply</div>	

Information feedback window
switch# show time-range

#### 4.8.6 ACL binding configuration.

Choose **ACL configuration > ACL binding configuration**, and the following page appears. There are "Attach ACL to port", "Show access group", "Clear PACL Statistic", "Attach ACL to vlan", "Show VACL configuration", "Clear vlan ACL statistic", configuration web pages.



##### 4.8.6.1 Attach ACL to port.

Choose **ACL configuration > ACL binding configuration > Attach ACL to port**, and the following page appears. You can attach an IP, MAC or MAC-IP ACL rule to a port, and decide whether to enable traffic-statistic.

Attach ACL to port	
Port	Ethernet1/0/1 ▼
ACL type	IP ▼
List name	<input type="text"/>
ACL Attached Direction	in ▼
Operation type	Add ▼
Apply	

#### 4.8.6.2 Show access group.

Choose **ACL configuration > ACL binding configuration > Show access group**, and the following page appears. You can show which ACL rules are attached to one port, or all the ACL and port binding status.

Show access group	
Port	ALL ▼
ACL Attached Direction	in ▼
Apply	

#### 4.8.6.3 Clear PACL Statistic.

Choose **ACL configuration > ACL binding configuration > Clear PACL Statistic**, and the following page appears. You can clear packet filter statistics at the specified port.

Clear PacL Statistic	
Port or Interface name	Ethernet1/0/1 ▼
ACL Attached Direction	in ▼
Apply	

#### 4.8.6.4 Attach ACL to vlan.

Choose **ACL configuration > ACL binding configuration > Attach ACL to vlan**, and the following page appears. You can attach an IP, MAC or MAC-IP ACL rule to a VLAN and decide whether to enable traffic-statistic.

Attach ACL to vlan	
VLAN interface	Vlan1 ▼
ACL type	IP ▼
List name	<input type="text"/>
ACL Attached Direction	in ▼
Operation type	Add ▼
Apply	

---

#### 4.8.6.5 Show VACL configuration.

Choose **ACL configuration > ACL binding configuration > Show VACL configuration**, and the following page appears. You can show which ACL rules are attached to a VLAN, or all the ACL and VLAN binding status.

show vACL configuration	
VLAN interface	Vlan1 ▾
ACL Attached Direction	in ▾
<div>Apply</div>	

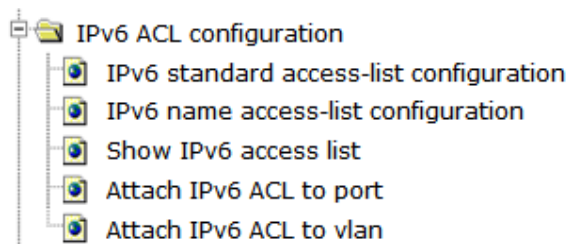
#### 4.8.6.6 Clear vlan ACL statistic.

Choose **ACL configuration > ACL binding configuration > Clear vlan ACL statistic**, and the following page appears. You can clear packet filter statistics at the specified VLAN.

clear vlan acl statistic	
VLAN interface	Vlan1 ▾
ACL Attached Direction	in ▾
<div>Apply</div>	

### 4.9 IPv6 ACL configuration.

Choose **IPv6 ACL configuration**, and the following page appears. There are "IPv6 standard access-list configuration", "IPv6 name access-list configuration", "Show IPv6 access list", "Attach IPv6 ACL to port", "Attach IPv6 ACL to vlan", configuration web pages.



#### 4.9.1 IPv6 standard access-list configuration.

Choose **IPv6 ACL configuration > IPv6 standard access-list configuration**, and the following page appears. You can add an IPv6 ACL rule to permit or deny data from

---

different source address. If the type is any -source don't need set IPv6 address, if the type is host-source fill a full IPv6 address, if the type is IPv6 source prefix the IPv6 address show fill a prefix.

IPv6 standard access-list configuration	
Access list number	<input type="text"/>
Rule	permit ▼
Source address type	host-source ▼
IPv6 address	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.9.2 IPv6 name access-list configuration.

Choose **IPv6 ACL configuration > IPv6 name access-list configuration**, and the following page appears. You can add an IPv6 ACL rule to permit or deny data from different source address. If the type is any -source don't need set IPv6 address, if the type is host-source fill a full IPv6 address, if the type is IPv6 source prefix the IPv6 address show fill a prefix. The List name must start with letter.

IPv6 name access-list configuration	
IPv6 name access-list	<input type="text"/>
Rule	▼
Source address type	host-source ▼
IPv6 address	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.9.3 Show IPv6 access list.

Choose **IPv6 ACL configuration > Show IPv6 access list**, and the following page appears. You can show the IPv6 ACL rule by List name or all the IPv6 ACL table by fill "all".

Show IPv6 access list	
List name	<input type="text"/>
<input type="button" value="Apply"/>	

#### 4.9.4 Attach IPv6 ACL to port.

Choose **IPv6 ACL configuration > Attach IPv6 ACL to port**, and the following page appears. You can attach an IPv6 ACL rule to a port, and decide whether to enable traffic-statistic.

Attach IPv6 ACL to port	
Port	Ethernet1/0/1 ▼
List name	<input type="text"/>
ACL Attached Direction	in ▼
Operation type	Add ▼
<input type="button" value="Apply"/>	

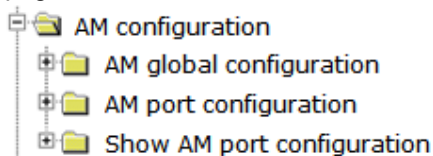
#### 4.9.5 Attach IPv6 ACL to vlan.

Choose **IPv6 ACL configuration > Attach IPv6 ACL to vlan**, and the following page appears. You can attach an IPv6 ACL rule to a VLAN, and decide whether to enable traffic-statistic.

Attach IPv6 ACL to vlan	
VLAN interface	Vlan1 ▼
List name	<input type="text"/>
ACL Attached Direction	in ▼
Operation type	Add ▼
<input type="button" value="Apply"/>	

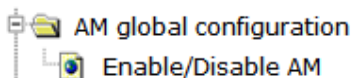
### 4.10 AM configuration.

Choose **AM configuration**, and the following page appears. There are "AM global configuration", "AM port configuration", "Show AM port configuration", configuration web pages.



#### 4.10.1 AM global configuration.

Choose **AM configuration > AM global configuration**, and the following page appears.



##### 4.10.1.1 Enable/Disable AM.

Choose **AM configuration > AM global configuration > Enable/Disable AM**, and the following page appears. You can enable or disable the AM function.

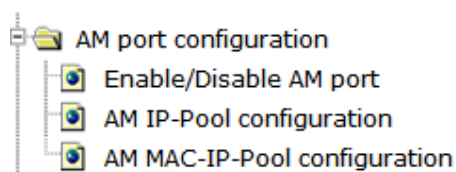


Enable/Disable AM	
AM status	Disable ▼
<input type="button" value="Apply"/>	

Information feedback window	
AM status	Disable

#### 4.10.2 AM port configuration.

Choose **AM configuration > AM port configuration**, and the following page appears. There are "Enable/Disable AM port", "AM IP-Pool configuration", "AM MAC-IP-Pool configuration", configuration web pages.



##### 4.10.2.1 Enable/Disable AM port.

Choose **AM configuration > AM port configuration > Enable/Disable AM port**, and the following page appears. You can enable or disable AM function for each port.

Enable/Disable AM port	
Port	AM port status
Ethernet1/0/1 ▼	Enable ▼
<input type="button" value="Apply"/>	

Information feedback window	
Port	AM port status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable
Ethernet1/0/10	Disable
Ethernet1/0/11	Disable
Ethernet1/0/12	Disable
Ethernet1/0/13	Disable
Ethernet1/0/14	Disable
Ethernet1/0/15	Disable
Ethernet1/0/16	Disable
Ethernet1/0/17	Disable

---

#### 4.10.2.2 AM IP-Pool configuration.

Choose **AM configuration > AM port configuration > AM IP-Pool configuration**, and the following page appears. You can set the IP pool start from the IP address and the count decide the number of continuous IP.

AM IP-Pool configuration	
Port	Ethernet1/0/1 ▾
IP address	<input type="text"/>
Count	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

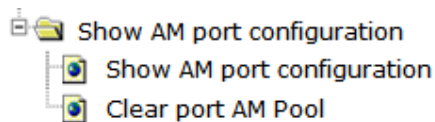
#### 4.10.2.3 AM MAC-IP-Poll configuration.

Choose **AM configuration > AM port configuration > AM MAC-IP-Poll configuration**, and the following page appears. You can set the MAC-IP address for each port, only data matched both MAC and IP address are permit.

AM MAC-IP-Pool configuration	
Port	Ethernet1/0/1 ▾
IP address	<input type="text"/>
MAC address	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

#### 4.10.3 Show AM port configuration.

Choose **AM configuration > Show AM port configuration**, and the following page appears. There are "Show AM port configuration", "Clear port", configuration web pages.



##### 4.10.3.1 Show AM port configuration.

Choose **AM configuration > Show AM port configuration > Show AM port configuration**, and the following page appears. You can show the AM rule for each port.

---

Show AM port configuration	
Port	<input type="text"/>
<input type="button" value="Apply"/>	

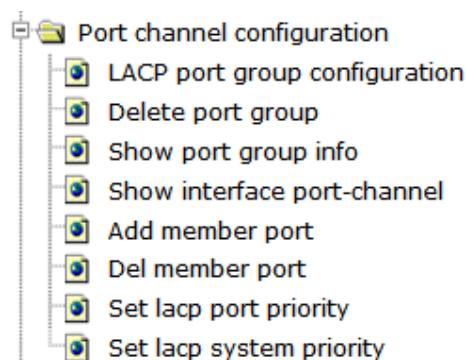
#### 4.10.3.2 Clear port configuration.

Choose **AM configuration > Show AM port configuration > Clear port configuration**, and the following page appears. You can clear the all the AM pool, ip pool or MAC-IP pool.

Clear port AM Pool	
Operation	<input type="text" value="all"/>
<input type="button" value="Apply"/>	

### 4.11 Port channel configuration.

Choose **Port channel configuration**, and the following page appears. There are "LACP port group configuration", "Delete port group", "Show port group info", "Show interface port-channel", "Add member port", "Del member port", "Set LACP port priority", "Set LACP system priority", configuration web pages.



#### 4.11.1 LACP port group configuration.

Choose **Port channel configuration > LACP port group configuration**, and the following page appears. You can set the LACP port group with the Load balance mode src-mac, dst-mac, dst-src-mac, src-IP, dst-ip, or dst-src-ip.

LACP port group configuration	
Group number	<input type="text"/>
Load balance mode	src-mac
<input type="button" value="set"/> <input type="button" value="Reset"/>	

Port group table					
Group number	Group member size	Load balance	Operation		
1	0	src-mac	<a href="#">Add member</a>	<a href="#">Remove member</a>	<a href="#">Show interface</a>

```

Information feedback window
switch# config
switch(config)# port-group 1 load-balance src-mac

```

## 4.11.2 Delete port group.

Choose **Port channel configuration > Delete port group**, and the following page appears. You can delete any rule in the Port group table.

Port group table			
Group number	Group member size	Load balance	Operation
1	0	src-mac	<a href="#">Delete</a>

## 4.11.3 Show port group info.

Choose **Port channel configuration > Show port group info**, and the following page appears. You can show the brief information and detail information of the port group function.

```

Information feedback window
switch# config
switch(config)# show port-group brief
ID: port group number; Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
      the first is selected ports number, the second is standby ports number, and
      the third is unselected ports number.
ID  Mode  Partner ID  Ports  Load-balance
-----
1   ,      ,      ,      src-mac
switch(config)# show port-group detail
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Port-group number: 1, Mode: , Load-balance: src-mac
Port-group detail information:
System ID: 0x8000,00-e0-53-16-d0-01
Local:
Port      Status  Priority  Oper-Key  Flag
-----
Remote:
Actor      Partner  Priority  Oper-Key  SystemID  Flag
-----

```

## 4.11.4 Show interface port-channel.

Choose **Port channel configuration > Show interface port-channel**, and the following page appears. You can show the brief and statistic information for every group number by click the “show interface” option.

LACP port group configuration	
Group number	<input type="text"/>
Load balance mode	src-mac
<input type="button" value="set"/> <input type="button" value="Reset"/>	

Port group table			
Group number	Group member size	Load balance	Operation
1	1	src-mac	<a href="#">Add member</a> <a href="#">Remove member</a> <a href="#">Show interface</a>

#### 4.11.5 Add member port.

Choose **Port channel configuration > Add member port**, and the following page appears. You can add a physical port to a port group via on, active or passive mode.

Port group add port	
Group number	1
Port list	Ethernet1/0/2
mode	on
<input type="button" value="Add"/> <input type="button" value="Reset"/>	

Port group port list	
Index	Port Name
1	Ethernet1/0/1

```

switch# config
switch(config)# interface Ethernet1/0/1
switch(config-if-ethernet1/0/1)# port-group 1 mode on

```

#### 4.11.6 Del member port.

Choose **Port channel configuration > Del member port**, and the following page appears. You can remove a physical port from a port group.

Port group remove port	
Group number	1
Port list	Ethernet1/0/1
<input type="button" value="Remove"/> <input type="button" value="Reset"/>	

Port group port list	
Index	Port Name
1	Ethernet1/0/1

#### 4.11.7 Set LACP port priority.

Choose **Port channel configuration > Set LACP port priority**, and the following page appears. You can set the LACP priority for the appointed port in a port group.

Set lacp port priority	
Group number	1 ▼
Port list	Ethernet1/0/1 ▼
Lacp port priority	
<input type="button" value="set"/> <input type="button" value="Reset"/>	

Port group port list	
Group number	Port Name
1	Ethernet1/0/1

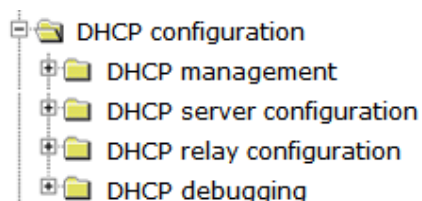
#### 4.11.8 Set LACP system priority.

Choose **Port channel configuration > Set LACP system priority**, and the following page appears. You can set the LACP system priority.

Set lacp system priority	
Lacp system priority	
<input type="button" value="set"/> <input type="button" value="Reset"/>	

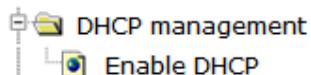
### 4.12 DHCP configuration.

Choose **DHCP configuration**, and the following page appears. There are "DHCP management", "DHCP server configuration", "DHCP relay configuration", "DHCP debugging", configuration web pages.



#### 4.12.1 DHCP management.

Choose **DHCP configuration > DHCP management**, and the following page appears.



#### 4.12.1.1 Enable DHCP.

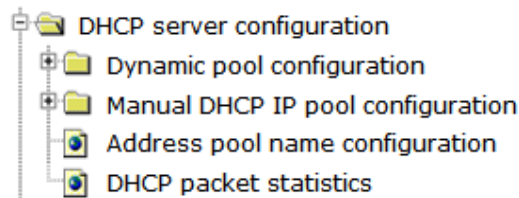
Choose **DHCP configuration > DHCP management > Enable DHCP**, and the following page appears. You can open or close the DHCP server and conflict logging function.

Enable DHCP	
DHCP server status	Close ▾
Conflict logging status	Open ▾
<input type="button" value="Apply"/>	

Information feedback window	
DHCP server status	Conflict logging status
Close	Open

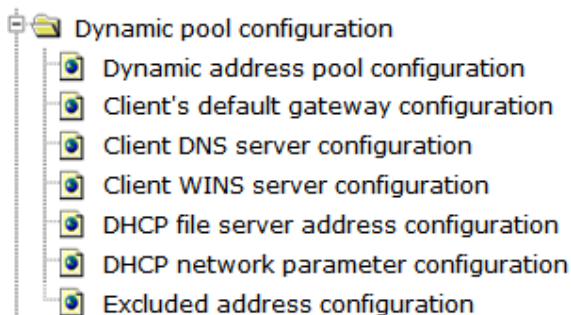
#### 4.12.2 DHCP server configuration.

Choose **DHCP configuration > DHCP server configuration**, and the following page appears. There are "Dynamic pool configuration", "Manual DHCP IP pool configuration", "Address pool name configuration", "DHCP packet statistics", configuration web pages.



##### 4.12.2.1 Dynamic pool configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration**, and the following page appears. There are "Dynamic address pool configuration", "Client's default gateway configuration", "Client DNS server configuration", "Client WINS server configuration", "DHCP file server address configuration", "DHCP network parameter configuration", "Excluded address configuration", configuration web pages.



##### 4.12.2.1.1 Dynamic address pool configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Dynamic address pool configuration**, and the following page appears. You can set a DHCP pool, the IP address and Network mask decide the address

range, the node type include b-node, p-node, m-node and h-node, and you can set the lease time.

DHCP IP address pool configuration	
DHCP pool name	<input type="text"/>
DHCP pool domain name	<input type="text"/>
Address range	IP address: <input type="text"/> Network mask: <input type="text"/>
DHCP client node type	b-node <input type="text"/>
Address lease timeout	<input type="radio"/> Infinite <input checked="" type="radio"/> Specified Day: <input type="text"/> Hour: <input type="text"/> Minute: <input type="text"/>
Operation	Add <input type="text"/>
Apply	

Information feedback window
switch# show ip dhcp pool config

#### 4.12.2.1.2 Client's default gateway configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Client's default gateway configuration**, and the following page appears.

You can set the default gateway for DHCP clients.

Client's default gateway configuration	
DHCP pool name	<input type="text"/>
Gateway 0	<input type="text"/>
Gateway 1	<input type="text"/>
Gateway 2	<input type="text"/>
Gateway 3	<input type="text"/>
Gateway 4	<input type="text"/>
Gateway 5	<input type="text"/>
Gateway 6	<input type="text"/>
Gateway 7	<input type="text"/>
Operation	Add <input type="text"/>
Apply	

#### 4.12.2.1.3 Client DNS server configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Client DNS server configuration**, and the following page appears.

You can set the DNS server address for DHCP client.



Client DNS server configuration	
DHCP pool name	▼
DNS server 0	
DNS server 1	
DNS server 2	
DNS server 3	
DNS server 4	
DNS server 5	
DNS server 6	
DNS server 7	
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.12.2.1.4 Client WINS server configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Client WINS server configuration**, and the following page appears. You can set the WINS server for DHCP clients.

Client WINS server configuration	
DHCP pool name	▼
WINS server 0	
WINS server 1	
WINS server 2	
WINS server 3	
WINS server 4	
WINS server 5	
WINS server 6	
WINS server 7	
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.12.2.1.5 DHCP file server address configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > DHCP file server address configuration**, and the following page appears. You can set the bootfile name and the supplied server IP address.

DHCP file server address configuration	
DHCP pool name	▼
DHCP client bootfile name	
File server 0	
File server 1	
File server 2	
File server 3	
File server 4	
File server 5	
File server 6	
File server 7	
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.12.2.1.6 DHCP network parameter configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > DHCP network parameter configuration**, and the following page appears. You can add option parameters for DHCP pool to complete the advanced function for DHCP, if not necessary don't configure.

DHCP network parameter configuration	
DHCP pool name	<input type="text"/>
Code	<input type="text"/>
Network parameter value type	IP ADDRESS <input type="text"/>
Network parameter value(ASCII,HEX or IP)	<input type="text"/>
Operation type	Add <input type="text"/>
<input type="button" value="Apply"/>	

#### 4.12.2.1.7 Excluded address configuration.

Choose **DHCP configuration > DHCP server configuration > Dynamic pool configuration > Excluded address configuration**, and the following page appears. You can set the excluded address for the DHCP pool address range.

Address allocation configuration	
Starting address	<input type="text"/>
Ending address	<input type="text"/>
Operation type	Add <input type="text"/>
<input type="button" value="Apply"/>	

Address list	
Starting address	Ending address
end of list	

#### 4.12.2.2 Manual DHCP IP pool configuration.

Choose **DHCP configuration > DHCP server configuration > Manual DHCP IP pool configuration**, and the following page appears.

<input type="checkbox"/> Manual DHCP IP pool configuration
<input type="checkbox"/> Static address pool configuration

##### 4.12.2.2.1 Static address pool configuration.

Choose **DHCP configuration > DHCP server configuration > Manual DHCP IP pool configuration > Static address pool configuration**, and the following page appears. You can set a hardware address with format rfc, ethernet or ieee802, and set a client IP address also, then the IP address will static to assign to the hardware address. And if you set a client IP address and client identifier, then the address will static to assign to the client with the identifier information.

Hardware address	
DHCP pool name	<input type="text"/>
Parameter choose	<input type="text"/>
Hardware address	<input type="text"/>
Operation	Add <input type="text"/>
<input type="button" value="Apply"/>	

Client pool configuration	
Client pool configuration	
Client IP address	<input type="text"/>
Client network mask	<input type="text"/>
Operation	Add <input type="text"/>
<input type="button" value="Apply"/>	

User name	
DHCP pool name	
User	<input type="text"/>
Client identifier	<input type="text"/>
Operation	Add <input type="text"/>
<input type="button" value="Apply"/>	

### 4.12.2.3 Address pool name configuration.

Choose **DHCP configuration > DHCP server configuration > Address pool name configuration**, and the following page appears. You can add a DHCP pool or remove a pool.

Address pool name configuration	
DHCP pool name	<input type="text"/>
Operation type	Add pool <input type="text"/>
<input type="button" value="Apply"/>	

Information feedback window	
switch# show ip dhcp pool config	

### 4.12.2.4 DHCP packet statistics.

Choose **DHCP configuration > DHCP server configuration > DHCP packet statistics**, and the following page appears. You can show the statistics information for DHCP.

DHCP packet statistics	
Address pool number	0
Proxy database	0
Dynamical assignment address	0
Manual binded address	0
Address conflict	0
Binding exceeding lease time	0
Errors	0

Received DHCP packet statistics	
Received	0
DHCP DISCOVER	0
DHCP REQUEST	0
DHCP DECLINE	0
DHCP RELEASE	0
DHCP INFORM	0

Transmitted DHCP packet statistics	
Transmitted	0
DHCP OFFER	0
DHCP ACK	0
DHCP NAK	0
DHCP RELAY	0
DHCP FORWARD	0

### 4.12.3 DHCP relay configuration.

Choose **DHCP configuration > DHCP relay configuration > DHCP relay configuration**, and the following page appears. You can set the DHCP forward range to 67 and set the DHCP server IP as the help-address.

DHCP forward UDP configuration	
Range	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Port

---

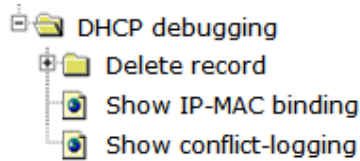
DHCP help-address configuration	
IP address	<input type="text"/>
L3 Interface	Vlan1 ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

IP address

L3 Interface

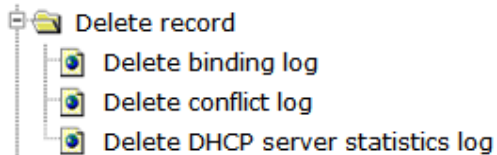
### 4.12.4 DHCP debugging.

Choose **DHCP configuration > DHCP debugging**, and the following page appears. There are "Delete record", "Show IP-MAC binding", "Show conflict-logging", configuration web pages.



#### 4.12.4.1 Delete record.

Choose **DHCP configuration > DHCP debugging > Delete record**, and the following page appears. There are "Delete binding log", "Delete conflict log", "Delete DHCP server statistics log", configuration web pages.



##### 4.12.4.1.1 Delete binding log.

Choose **DHCP configuration > DHCP debugging > Delete record > Delete binding log**, and the following page appears. You can delete the record of one IP address binding with hardware address, or delete all binding table.

Delete DHCP binding log	
Delete binding area	Delete all binding log ▼
IP Address	<input type="text"/>
<input type="button" value="Apply"/>	

##### 4.12.4.1.2 Delete conflict log.

Choose **DHCP configuration > DHCP debugging > Delete record > Delete conflict log**, and the following page appears. You can delete the conflict log of one IP address or delete all conflict log.

Delete conflict log	
Delete conflict address area	Delete all conflict log ▼
IP Address	<input type="text"/>
<input type="button" value="Apply"/>	

##### 4.12.4.1.3 Delete DHCP server statistics log.

Choose **DHCP configuration > DHCP debugging > Delete record > Delete DHCP server statistics log**, and the following page appears. You can remove the DHCP server statistics logging.

Delete DHCP server statistics log
<input type="button" value="Apply"/>

---

#### 4.12.4.2 Show IP-MAC binding.

Choose **DHCP configuration > DHCP debugging > Show IP-MAC binding**, and the following page appears. You can show the IP and hardware address binding information.

```
Information feedback window
switch# clear ip dhcp server statistics
switch# show ip dhcp binding
Total dhcp binding items: 0, the matched: 0
IP address      Hardware address  Lease expiration  Type
```

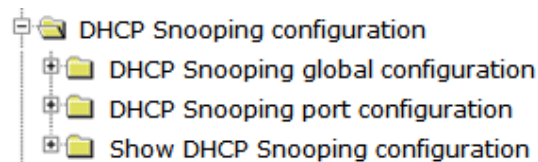
#### 4.12.4.3 Show conflict-logging.

Choose **DHCP configuration > DHCP debugging > Show conflict-logging**, and the following page appears. You can show the DHCP conflict information.

```
Information feedback window
switch# show ip dhcp conflict
IP Address      Detection method  Detection Time
```

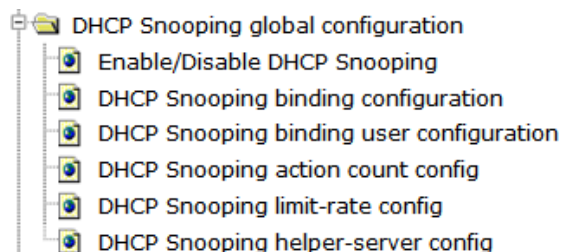
### 4.13 DHCP Snooping configuration.

Choose **DHCP Snooping configuration**, and the following page appears. There are "DHCP Snooping global configuration", "DHCP Snooping port configuration", "Show DHCP Snooping configuration", configuration web pages.



#### 4.13.1 DHCP Snooping global configuration.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration**, and the following page appears. There are "Enable/Disable DHCP Snooping", "DHCP Snooping binding configuration", "DHCP Snooping binding user configuration", "DHCP Snooping action count config", "DHCP Snooping limit-rate config", "DHCP Snooping helper-server config", configuration web pages.



---

#### 4.13.1.1 Enable/Disable DHCP Snooping.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > Enable/Disable DHCP Snooping**, and the following page appears. You can enable or disable the DHCP Snooping function.

Enable/Disable DHCP Snooping	
DHCP Snooping status	Disable ▾
<div>Apply</div>	

Information feedback window	
DHCP Snooping status	Disable

#### 4.13.1.2 DHCP Snooping binding configuration.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping binding configuration**, and the following page appears. You can enable or disable the DHCP Snooping binding function.

Enable/Disable DHCP Snooping binding	
DHCP Snooping binding status	Disable ▾
<div>Apply</div>	

Information feedback window	
DHCP Snooping binding status	Disable

#### 4.13.1.3 DHCP Snooping binding user configuration.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping binding user configuration**, and the following page appears. You can bind the MAC address, IP address, VLAN ID and port for a client.

DHCP Snooping binding user configuration	
MAC address	<input type="text"/>
User IP address	<input type="text"/>
User mask	<input type="text"/>
VLAN ID	<input type="text"/>
Port	Ethernet1/0/1 ▾
Operation	Add ▾
<div>Apply</div>	

---

#### 4.13.1.4 DHCP Snooping action count config.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping action count config**, and the following page appears. You can set the count of the DHCP Snooping action.

DHCP Snooping action count config	
DHCP Snooping action count	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Information feedback window	
DHCP Snooping action count	10

#### 4.13.1.5 DHCP Snooping limit-rate config.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping limit-rate config**, and the following page appears. You can set the count of the request and reply packets transmitting per second.

DHCP Snooping limit-rate config	
Packet per second	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Information feedback window	
Packet per second	100

#### 4.13.1.6 DHCP Snooping helper-server config.

Choose **DHCP Snooping configuration > DHCP Snooping global configuration > DHCP Snooping helper-server config**, and the following page appears. You can set the helper-server address to save binding information detected by switch. The UDP port default is 9119, and local IP address should be the management IP of switch, you can choose the server as the primary or secondary server.

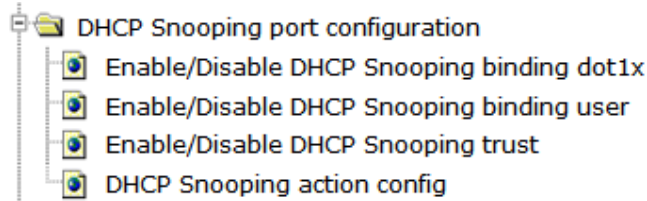
DHCP Snooping helper-server config	
Helper-server address	<input type="text"/>
Helper-server UDP port	<input type="text"/>
Local IP address	<input type="text"/>
Second address	▼
Operation	Add ▼
<input type="button" value="Apply"/>	



---

### 4.13.2 DHCP Snooping port configuration.

Choose **DHCP Snooping configuration**, and the following page appears. There are "Enable/Disable DHCP Snooping binding dot1x", "Enable/Disable DHCP Snooping binding user", "Enable/Disable DHCP Snooping trust", "DHCP Snooping action config", configuration web pages.



#### 4.13.2.1 Enable/Disable DHCP Snooping binding dot1x.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > Enable/Disable DHCP Snooping binding dot1x**, and the following page appears. You can enable or disable DHCP Snooping binding dot1x function for each port.

Enable/Disable DHCP Snooping binding dot1x	
Port	DHCP Snooping binding dot1x status
Ethernet1/0/1	Enable

Information feedback window	
Port	DHCP Snooping binding dot1x status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable
Ethernet1/0/10	Disable
Ethernet1/0/11	Disable
Ethernet1/0/12	Disable

#### 4.13.2.2 Enable/Disable DHCP Snooping binding user.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > Enable/Disable DHCP Snooping binding user**, and the following page appears. You can enable or disable the DHCP Snooping binding user function for each port.

Enable/Disable DHCP Snooping binding user	
Port	DHCP Snooping binding user status
Ethernet1/0/1 ▼	Enable ▼
<input type="button" value="Apply"/>	

Information feedback window	
Port	DHCP Snooping binding user status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable

#### 4.13.2.3 Enable/Disable DHCP Snooping trust.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > Enable/Disable DHCP Snooping trust**, and the following page appears. You can enable or disable DHCP Snooping binding trust function for each port.

Enable/Disable DHCP Snooping trust	
Port	DHCP Snooping binding trust status
Ethernet1/0/1 ▼	Enable ▼
<input type="button" value="Apply"/>	

Information feedback window	
Port	DHCP Snooping binding trust status
Ethernet1/0/1	Disable
Ethernet1/0/2	Disable
Ethernet1/0/3	Disable
Ethernet1/0/4	Disable
Ethernet1/0/5	Disable
Ethernet1/0/6	Disable
Ethernet1/0/7	Disable
Ethernet1/0/8	Disable
Ethernet1/0/9	Disable
Ethernet1/0/10	Disable
Ethernet1/0/11	Disable

#### 4.13.2.4 DHCP Snooping action config.

Choose **DHCP Snooping configuration > DHCP Snooping configuration > DHCP Snooping action config**, and the following page appears. You can choose shutdown or blackhole the port while invalid DHCP packet detected, and the recover time.

DHCP Snooping action config	
Port	Ethernet1/0/1 ▾
DHCP Snooping action	shutdown ▾
DHCP Snooping recovery time	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window		
Port	DHCP Snooping action	DHCP Snooping recovery time
Ethernet1/0/1	none	0
Ethernet1/0/2	none	0
Ethernet1/0/3	none	0
Ethernet1/0/4	none	0
Ethernet1/0/5	none	0
Ethernet1/0/6	none	0
Ethernet1/0/7	none	0
Ethernet1/0/8	none	0
Ethernet1/0/9	none	0
Ethernet1/0/10	none	0
Ethernet1/0/11	none	0

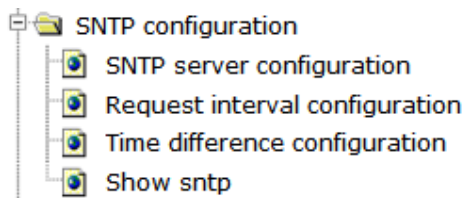
### 4.13.3 Show DHCP Snooping configuration.

Choose **DHCP Snooping configuration > Show DHCP Snooping configuration > Show DHCP Snooping configuration**, and the following page appears. You can show the DHCP Snooping information for one port or all ports.

Show DHCP Snooping configuration	
DHCP Snooping show object	▾
<input type="button" value="Apply"/>	

## 4.14 SNTP configuration.

Choose **SNTP configuration**, and the following page appears. There are "SNTP server configuration", "Request interval configuration", "Time difference configuration", "Show SNTP", configuration web pages.



### 4.14.1 SNTP server configuration.

Choose **SNTP configuration > SNTP server configuration**, and the following page appears. You can set the SNTP server address and client version.

SNTP server and version configuration	
Server address	<input type="text"/>
Version	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.14.2 Request interval configuration.

Choose **SNTP configuration > Request interval configuration**, and the following page appears. You can set the time interval that the client send request.

Request interval from SNTP client to SNTP server	
Interval	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

Interval	
Interval	64

#### 4.14.3 Time difference configuration.

Choose **SNTP configuration > Time difference configuration**, and the following page appears. You can set the Time zone, and add or subtract a value from the time obtain from server.

Time difference configuration	
Time zone	<input type="text"/>
Time difference	<input checked="" type="radio"/> After-utc <input type="radio"/> Before-utc
Time value	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.14.4 Show SNTP.

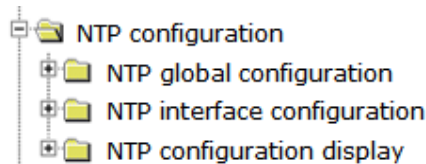
Choose **SNTP configuration > Show SNTP**, and the following page appears. You can show the detail information for SNIP.

Information feedback window	
<pre>switch# config t switch(config)# show sntp server address          version last receive</pre>	

---

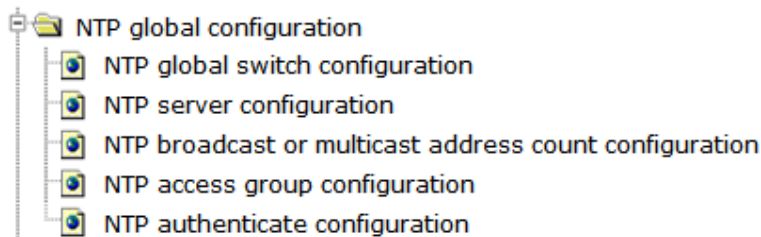
## 4.15 NTP configuration.

Choose **NTP configuration**, and the following page appears. There are "NTP global configuration", "NTP interface configuration", "NTP configuration", configuration web pages.



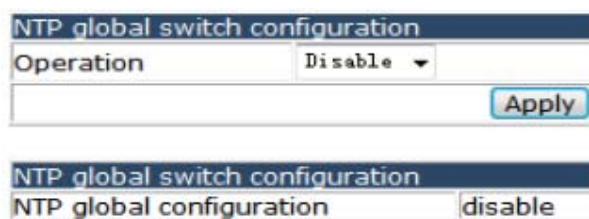
### 4.15.1 NTP global configuration.

Choose **NTP configuration > NTP global configuration**, and the following page appears. There are "NTP global switch configuration", "NTP server configuration", "NTP broadcast or multicast address count configuration", "NTP access group configuration", "NTP authenticate configuration", configuration web pages.



#### 4.15.1.1 NTP global switch configuration.

Choose **NTP configuration > NTP global configuration > NTP global switch configuration**, and the following page appears. You can enable or disable the NTP global switch function.



#### 4.15.1.2 NTP server configuration.

Choose **NTP configuration > NTP global configuration > NTP server configuration**, and the following page appears. You can set the NTP server address, version and key parameters.

NTP server and version configuration	
Server address	<input type="text"/>
Version	<input type="text"/>
Key	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

```

Information feedback window
switch# config t
switch(config)# show ntp session
ntp peer doesn't exist!

```

#### 4.15.1.3 NTP broadcast or multicast address count configuration.

Choose **NTP configuration > NTP global configuration > NTP broadcast or multicast address count configuration**, and the following page appears, You can set the max count of the NTP broadcast or multicast address.

NTP broadcast or multicast address count configuration	
Address max count	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Address max count	
Address max count	50

#### 4.15.1.4 NTP access group configuration.

Choose **NTP configuration > NTP global configuration > NTP access group configuration**, and the following page appears. You can set a access list for NTP.

NTP access group configuration	
Access list	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Access list	
-------------	--

#### 4.15.1.5 NTP authenticate configuration.

Choose **NTP configuration > NTP global configuration > NTP authenticate configuration**, and the following page appears. You can set authentication-key, trust-key or without key for NTP authenticate.

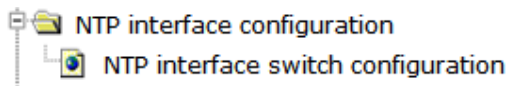
NTP authenticate configuration	
NTP authenticate switch	Disable ▾
Key type	none ▾
Key	<input type="text"/>
MD5	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Access list

Information feedback window  
no ntp authenticate

## 4.15.2 NTP interface configuration.

Choose **NTP configuration**, and the following page appears. There are "NTP interface switch configuration", configuration web pages.



### 4.15.2.1 NTP interface switch configuration.

Choose **NTP configuration > NTP interface switch configuration**, and the following page appears. You can set the NTP FOR VLAN, the NTP interface client include none, broadcast, no broadcast, multicast, no multicast, IPv6 multicast, no NTP interface IPv6 multicast.

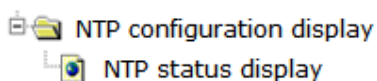
NTP interface configuration	
VLAN interface	Vlan1 ▾
NTP interface configuration	Disable ▾
NTP interface client	none ▾
<input type="button" value="Apply"/>	

NTP interface configuration

Information feedback window  
Interface name:Vlan1

## 4.15.3 NTP configuration display.

Choose **NTP configuration**, and the following page appears. There are "NTP status display", configuration web pages.



---

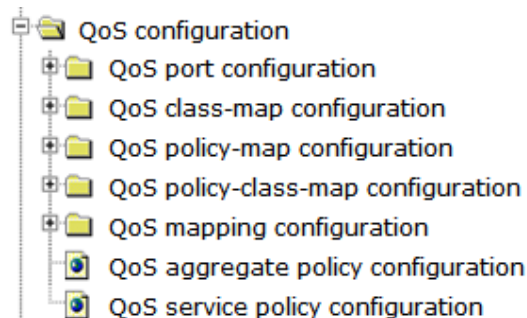
#### 4.15.3.1 NTP status display.

Choose **NTP configuration > NTP status display**, and the following page appears. You can show the NTP status.

```
Information feedback window
switch# show ntp status
ntp clock status: unsynchronized
```

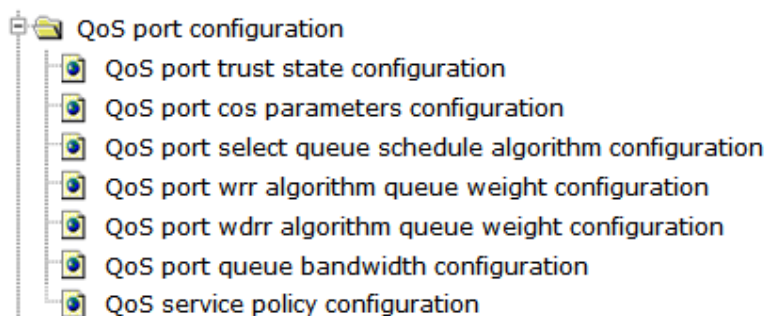
#### 4.16 QoS configuration.

Choose **QoS configuration**, and the following page appears. There are "QoS port configuration", "QoS class-map configuration", "QoS policy-map configuration", "QoS policy-class-map configuration", "QoS mapping configuration", "QoS aggregate policy", "QoS service policy configuration", configuration web pages.



##### 4.16.1 QoS port configuration.

Choose **QoS configuration > QoS port configuration**, and the following page appears. There are "QoS port trust state configuration", "QoS port cos parameters configuration", "QoS port select queue schedule algorithm configuration", "QoS port WRR algorithm queue weight configuration", "QoS port WDRR algorithm queue weight configuration", "QoS port queue bandwidth configuration", "QoS service policy configuration", configuration web pages.





#### 4.16.1.1 QoS port trust state configuration.

Choose **QoS configuration > QoS port configuration > QoS port trust state configuration**, and the following page appears. You can set the QoS trust packet class to cos or dscp for each port.

QoS port trust state configuration	
Port	Ethernet1/0/1 ▾
Packet class rule	COS ▾
Operation	Add ▾
<div>Apply</div>	

Information feedback window	
Port	Trust class
Ethernet1/0/1	COS
Ethernet1/0/2	COS
Ethernet1/0/3	COS
Ethernet1/0/4	COS
Ethernet1/0/5	COS
Ethernet1/0/6	COS
Ethernet1/0/7	COS
Ethernet1/0/8	COS
Ethernet1/0/9	COS
Ethernet1/0/10	COS
Ethernet1/0/11	COS
Ethernet1/0/12	COS

#### 4.16.1.2 QoS port cos parameters configuration.

Choose **QoS configuration > QoS port configuration > QoS port COS parameters configuration**, and the following page appears. You can set the default COS value for each port.

QoS port cos parameters configuration	
Port	Ethernet1/0/1 ▾
Port related COS value	<input type="text"/>
Operation	Add ▾
<div>Apply</div>	

Information feedback window	
Port	Port related COS value
Ethernet1/0/1	0
Ethernet1/0/2	0
Ethernet1/0/3	0
Ethernet1/0/4	0
Ethernet1/0/5	0
Ethernet1/0/6	0
Ethernet1/0/7	0
Ethernet1/0/8	0
Ethernet1/0/9	0
Ethernet1/0/10	0
Ethernet1/0/11	0
Ethernet1/0/12	0

---

#### 4.16.1.3 QoS port select queue schedule algorithm configuration.

Choose **QoS configuration > QoS port configuration > QoS port select queue schedule algorithm configuration**, and the following page appears. You can set the QoS queue schedule algorithm to sp, wrr or wdrp mode.

QoS port select queue schedule algorithm configuration	
Port	Ethernet1/0/1 ▾
Queue schedule algorithm	sp ▾
<div>Apply</div>	

Information feedback window	
Port	Trust class
Ethernet1/0/1	wrr
Ethernet1/0/2	wrr
Ethernet1/0/3	wrr
Ethernet1/0/4	wrr
Ethernet1/0/5	wrr
Ethernet1/0/6	wrr
Ethernet1/0/7	wrr
Ethernet1/0/8	wrr
Ethernet1/0/9	wrr
Ethernet1/0/10	wrr
Ethernet1/0/11	wrr
Ethernet1/0/12	wrr
Ethernet1/0/13	wrr
Ethernet1/0/14	wrr
Ethernet1/0/15	wrr

#### 4.16.1.4 QoS port WRR algorithm queue weight configuration.

Choose **QoS configuration > QoS port configuration > QoS port WRR algorithm queue weight configuration**, and the following page appears. You can set the WRR queue Weight value for each port.

QoS port wrr algorithm queue weight configuration	
Port	Ethernet1/0/1 ▾
Weight1	<input type="text"/>
Weight2	<input type="text"/>
Weight3	<input type="text"/>
Weight4	<input type="text"/>
Weight5	<input type="text"/>
Weight6	<input type="text"/>
Weight7	<input type="text"/>
Weight8	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window	
Port	Queue weight
Ethernet1/0/1	1 2 3 4 5 6 7 8
Ethernet1/0/2	1 2 3 4 5 6 7 8
Ethernet1/0/3	1 2 3 4 5 6 7 8
Ethernet1/0/4	1 2 3 4 5 6 7 8
Ethernet1/0/5	1 2 3 4 5 6 7 8
Ethernet1/0/6	1 2 3 4 5 6 7 8
Ethernet1/0/7	1 2 3 4 5 6 7 8

#### 4.16.1.5 QoS port WDRR algorithm queue weight configuration.

Choose **QoS configuration > QoS port configuration > QoS port WDRR algorithm queue weight configuration**, and the following page appears. You can set the WDRR queue Weight value for each port.

QoS port wdr algorithm queue weight configuration	
Port	Ethernet1/0/1 ▾
Weight1	<input type="text"/>
Weight2	<input type="text"/>
Weight3	<input type="text"/>
Weight4	<input type="text"/>
Weight5	<input type="text"/>
Weight6	<input type="text"/>
Weight7	<input type="text"/>
Weight8	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window	
Port	Queue weight
Ethernet1/0/1	16 32 64 128 256 512 1024 1024
Ethernet1/0/2	16 32 64 128 256 512 1024 1024
Ethernet1/0/3	16 32 64 128 256 512 1024 1024
Ethernet1/0/4	16 32 64 128 256 512 1024 1024
Ethernet1/0/5	16 32 64 128 256 512 1024 1024
Ethernet1/0/6	16 32 64 128 256 512 1024 1024
Ethernet1/0/7	16 32 64 128 256 512 1024 1024
Ethernet1/0/8	16 32 64 128 256 512 1024 1024
Ethernet1/0/9	16 32 64 128 256 512 1024 1024
Ethernet1/0/10	16 32 64 128 256 512 1024 1024

---

#### 4.16.1.6 QoS port queue bandwidth configuration.

Choose **QoS configuration > QoS port configuration > QoS port queue bandwidth configuration**, and the following page appears. You can set the MinBandwidth and MaxBandwidth value for different Queue of each port.

QoS port queue bandwidth configuration	
Port	Ethernet1/0/1 ▾
Queue id	<input type="text"/>
MinBandwidth	<input type="text"/>
MaxBandwidth	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window			
Port	Queue id	MinBandwidth	MaxBandwidth

#### 4.16.1.7 QoS service policy configuration.

Choose **QoS configuration > QoS port configuration > QoS service policy configuration**, and the following page appears. You can mapping a policy-map to a physical port, the policy map setting refer to QoS policy-map configuration.

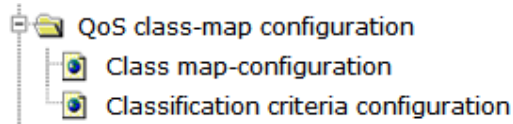
QoS service policy configuration	
Port	Ethernet1/0/1 ▾
Policy map name	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window	
Port	Policy map name
Ethernet1/0/1	none
Ethernet1/0/2	none
Ethernet1/0/3	none
Ethernet1/0/4	none
Ethernet1/0/5	none
Ethernet1/0/6	none
Ethernet1/0/7	none
Ethernet1/0/8	none
Ethernet1/0/9	none
Ethernet1/0/10	none
Ethernet1/0/11	none
Ethernet1/0/12	none
Ethernet1/0/13	none
Ethernet1/0/14	none

---

## 4.16.2 QoS class-map configuration.

Choose **QoS configuration > QoS class-map configuration**, and the following page appears. There are "Class map-configuration", "Classification criteria configuration", configuration web pages.



### 4.16.2.1 Class map-configuration.

Choose **QoS configuration > QoS class-map configuration > Class map-configuration**, and the following page appears. You can add a Class-map rule.

Class map-configuration	
Class-map name	<input type="text"/>
Operation	Add ▼
<div>Apply</div>	

Information feedback window

### 4.16.2.2 Classification criteria configuration.

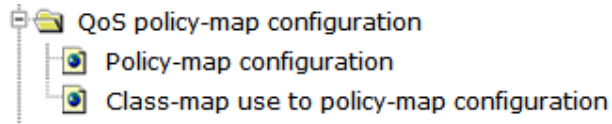
Choose **QoS configuration > QoS class-map configuration > Classification criteria configuration**, and the following page appears. You can set the matching criteria for the class-map table. The classification criteria rule include access-group, IP-dscp, IP Precedence, Vlan, COS, C-Vlan, IPv6-dscp, IPv6-flowlabel.

Classification criteria configuration	
Classification criteria rule	access-group ▼
Class-map name	▼ <input type="text"/>
ACL list name	<input type="text"/>
Operation	Add ▼
<div>Apply</div>	

---

### 4.16.3 QoS policy-map configuration.

Choose **QoS configuration > QoS policy-map configuration**, and the following page appears. There are "Policy map-configuration", "Class-map use to policy-map configuration", configuration web pages.



#### 4.16.3.1 Policy-map configuration.

Choose **QoS configuration > QoS policy-map configuration > Policy-map configuration**, and the following page appears. You can add a Policy-map rule.

Policy-map configuration	
Policy-map name	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="text"/>	
<input type="button" value="Apply"/>	

Information feedback window

#### 4.16.3.2 Class-map use to policy-map configuration.

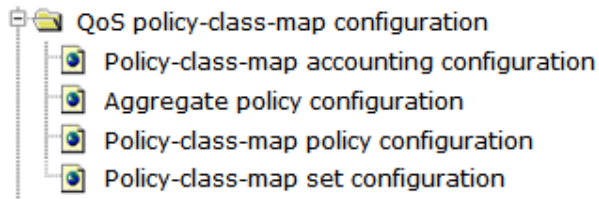
Choose **QoS configuration > QoS policy-map configuration > Class-map use to policy-map configuration**, and the following page appears. You can configure the class-map use to policy-map.

Class-map use to policy-map configuration	
Policy-map name	<input type="text"/>
Class-map name	<input type="text"/>
Inserted before the class-map name	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="text"/>	
<input type="button" value="Apply"/>	

Information feedback window
Policy-map name <input type="text"/> Class-map name <input type="text"/>

#### 4.16.4 QoS policy-class-map configuration.

Choose **QoS configuration > QoS policy-class-map configuration**, and the following page appears. There are "Policy-class-map accounting configuration", "Aggregate policy configuration", "Policy-class-map policy configuration", "Policy-class-map set configuration", configuration web pages.



#### 4.16.4.1 Policy-class-map accounting configuration.

Choose **QoS configuration > QoS policy-class-map configuration > Policy-class-map accounting configuration**, and the following page appears. You can enable or disable the policy-class-map.

Policy-class-map accounting configuration	
Policy-map name	<input type="text"/>
Class-map name	<input type="text"/>
Accounting switch	Disable <input type="text"/>
<input type="button" value="Apply"/>	

Information feedback window		
Policy-map name	Class-map name	Accounting switch

#### 4.16.4.2 Aggregate policy configuration.

Choose **QoS configuration > QoS policy-class-map configuration > Aggregate policy configuration**, and the following page appears. You can set the Aggregate policy.

Aggregate policy configuration	
Policy-map name	<input type="text"/>
Class-map name	<input type="text"/>
Aggregate policy name	<input type="text"/>
Operation	Add <input type="text"/>
<input type="button" value="Apply"/>	

Information feedback window		
Policy-map name	Class-map name	Aggregate policy name

#### 4.16.4.3 Policy-class-map policy configuration.

Choose **QoS configuration > QoS policy-class-map configuration > Policy-class-map policy configuration**, and the following page appears. You can set the policy-class-map policy.

Policy-class-map policy configuration	
Policy-map name	test2 ▾
Class-map name	test ▾
Committed information rate	<input type="text"/>
Committed burst size	<input type="text"/>
Peak information rate	<input type="text"/>
Peak burst size	<input type="text"/>
Conform action	<input type="checkbox"/> drop <input type="checkbox"/> transmit <input type="checkbox"/> set-dscp-transmit <input type="text"/> <input type="checkbox"/> set-prec-transmit <input type="text"/> <input type="checkbox"/> set-cos-transmit <input type="text"/> <input type="checkbox"/> set-internal-priority <input type="text"/> <input type="checkbox"/> set-Drop-Precedence <input type="text"/>
Exceed action	<input type="checkbox"/> drop <input type="checkbox"/> transmit <input type="checkbox"/> set-dscp-transmit <input type="text"/> <input type="checkbox"/> set-prec-transmit <input type="text"/> <input type="checkbox"/> set-cos-transmit <input type="text"/> <input type="checkbox"/> set-internal-priority <input type="text"/> <input type="checkbox"/> set-Drop-Precedence <input type="text"/>
Violated action	<input type="checkbox"/> drop <input type="checkbox"/> transmit <input type="checkbox"/> set-dscp-transmit <input type="text"/> <input type="checkbox"/> set-prec-transmit <input type="text"/> <input type="checkbox"/> set-cos-transmit <input type="text"/> <input type="checkbox"/> set-internal-priority <input type="text"/> <input type="checkbox"/> set-Drop-Precedence <input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

#### 4.16.4.4 Policy-class-map set configuration.

Choose **QoS configuration > QoS policy-class-map configuration >**

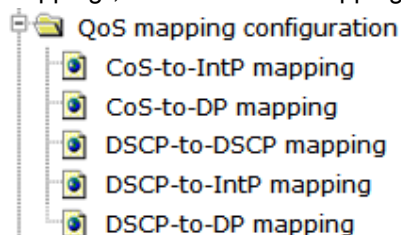


**Policy-class-map set configuration**, and the following page appears. You can set new classification criteria rule for classified traffic. The rule include IP DSCP, IP precedence, DROP precedence, Internal Priority, COS, C-vid, S-vid.

Classification criteria configuration	
Classification criteria rule	ip dscp ▼
Policy-map name	▼
Class-map name	▼
DSCP	
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.16.5 QoS mapping configuration.

Choose **QoS configuration > QoS mapping configuration**, and the following page appears. There are "COS-to-IntP mapping", "COS-to-DP mapping", "DSCP-to-DSCP mapping", "DSCP-to-IntP mapping", "DSCP-to-DP mapping", configuration web pages.



##### 4.16.5.1 COS-to-IntP mapping.

Choose **QoS configuration > QoS mapping configuration > COS-to-IntP mapping**, and the following page appears. You can set the mapping COS-to-IntP.

CoS-to-IntP mapping								
CoS value	0	1	2	3	4	5	6	7
IntP value	0	1	2	3	4	5	6	7
Operation type	Configuration ▼							
<input type="button" value="Apply"/>								

```

Information feedback window
Switch# config t
Switch(config)# show mls qos map cos-intp
Ingress COS-TO-Internal-Priority map:
COS:  0   1   2   3   4   5   6   7
-----
INTP: 0   1   2   3   4   5   6   7

```

#### 4.16.5.2 COS-to-IntP mapping.

Choose **QoS configuration > QoS mapping configuration > COS-to-DP mapping**, and the following page appears. You can set the mapping COS-to-DP.

CoS-to-DP mapping								
CoS value	0	1	2	3	4	5	6	7
DP value	0	0	0	0	0	0	0	0
Operation type	Configuration ▼							
<div>Apply</div>								

```
Information feedback window
Switch# config t
Switch(config)# show mls qos map cos-dp
Ingress COS-TO-Drop-Precedence map:
COS:  0   1   2   3   4   5   6   7
-----
DP:   0   0   0   0   0   0   0   0
```

#### 4.16.5.3 DSCP-to-DSCP mapping.

Choose **QoS configuration > QoS mapping configuration > DSCP-to-DSCP mapping**, and the following page appears. You can set the mapping DSCP-to-DSCP.

DSCP-to-DSCP mapping	
DSCP value1	<input type="text"/>
DSCP value2(optional)	<input type="text"/>
DSCP value3(optional)	<input type="text"/>
DSCP value4(optional)	<input type="text"/>
DSCP value5(optional)	<input type="text"/>
DSCP value6(optional)	<input type="text"/>
DSCP value7(optional)	<input type="text"/>
DSCP value8(optional)	<input type="text"/>
DSCP value	<input type="text"/>
Operation type	Configuration ▼
<div>Apply</div>	

```
Information feedback window
Switch# config t
Switch(config)# show mls qos map dscp-dscp
Ingress DSCP-TO-DSCP map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:      0   0   0   0   0   0   0   0   0   8
1:      8   8   8   8   8   8  16  16  16  16
2:     16  16  16  16  24  24  24  24  24  24
3:     24  24  32  32  32  32  32  32  32  32
4:     40  40  40  40  40  40  40  40  48  48
5:     48  48  48  48  48  48  56  56  56  56
6:     56  56  56  56
```

#### 4.16.5.4 DSCP-to-IntP mapping.

Choose **QoS configuration > QoS mapping configuration > DSCP-to-IntP mapping**, and the following page appears. You can set the mapping DSCP-to-IntP.

DSCP-to-IntP mapping	
DSCP value1	<input type="text"/>
DSCP value2(optional)	<input type="text"/>
DSCP value3(optional)	<input type="text"/>
DSCP value4(optional)	<input type="text"/>
DSCP value5(optional)	<input type="text"/>
DSCP value6(optional)	<input type="text"/>
DSCP value7(optional)	<input type="text"/>
DSCP value8(optional)	<input type="text"/>
IntP value	<input type="text"/>
Operation type	Configuration ▾
<input type="button" value="Apply"/>	

```
Information feedback window
Switch# config t
Switch(config)# show mls qos map dscp-intp
Ingress DSCP-TO-Internal-Priority map:
d1 : d2  0  1  2  3  4  5  6  7  8  9
0:      0  0  0  0  0  0  0  0  0  1  1
1:      1  1  1  1  1  1  2  2  2  2
2:      2  2  2  2  3  3  3  3  3  3
3:      3  3  4  4  4  4  4  4  4  4
4:      5  5  5  5  5  5  5  5  6  6
5:      6  6  6  6  6  6  7  7  7  7
6:      7  7  7  7
```

#### 4.16.5.5 DSCP-to-DP mapping.

Choose **QoS configuration > QoS mapping configuration > DSCP-to-DP mapping**, and the following page appears. You can set the mapping DSCP-to-DP.

DSCP-to-DP mapping	
DSCP value1	<input type="text"/>
DSCP value2(optional)	<input type="text"/>
DSCP value3(optional)	<input type="text"/>
DSCP value4(optional)	<input type="text"/>
DSCP value5(optional)	<input type="text"/>
DSCP value6(optional)	<input type="text"/>
DSCP value7(optional)	<input type="text"/>
DSCP value8(optional)	<input type="text"/>
DP value	<input type="text"/>
Operation type	Configuration ▾
<input type="button" value="Apply"/>	

```
Information feedback window
Switch# config t
Switch(config)# show mls qos map dscp-dp
Ingress DSCP-TO-Drop-Precedence map:
d1 : d2  0  1  2  3  4  5  6  7  8  9
0:      0  0  0  0  0  0  0  0  0  0
1:      0  0  0  0  0  0  0  0  0  0
2:      0  0  0  0  0  0  0  0  0  0
3:      0  0  0  0  0  0  0  0  0  0
4:      0  0  0  0  0  0  0  0  0  0
5:      0  0  0  0  0  0  0  0  0  0
6:      0  0  0  0
```

---

#### 4.16.6 QoS aggregate policy configuration.

Choose **QoS configuration > QoS aggregate policy**, and the following page appears.  
You can set QoS-aggregate-policy strategy. You can set the QoS aggregate policy.

Policy-class-map policy configuration	
Policy-map name	test2 ▾
Class-map name	test ▾
Committed information rate	<input type="text"/>
Committed burst size	<input type="text"/>
Peak information rate	<input type="text"/>
Peak burst size	<input type="text"/>
Conform action	<input type="checkbox"/> drop <input type="checkbox"/> transmit <input type="checkbox"/> set-dscp-transmit <input type="text"/> <input type="checkbox"/> set-prec-transmit <input type="text"/> <input type="checkbox"/> set-cos-transmit <input type="text"/> <input type="checkbox"/> set-internal-priority <input type="text"/> <input type="checkbox"/> set-Drop-Precedence <input type="text"/>
Exceed action	<input type="checkbox"/> drop <input type="checkbox"/> transmit <input type="checkbox"/> set-dscp-transmit <input type="text"/> <input type="checkbox"/> set-prec-transmit <input type="text"/> <input type="checkbox"/> set-cos-transmit <input type="text"/> <input type="checkbox"/> set-internal-priority <input type="text"/> <input type="checkbox"/> set-Drop-Precedence <input type="text"/>
Violated action	<input type="checkbox"/> drop <input type="checkbox"/> transmit <input type="checkbox"/> set-dscp-transmit <input type="text"/> <input type="checkbox"/> set-prec-transmit <input type="text"/> <input type="checkbox"/> set-cos-transmit <input type="text"/> <input type="checkbox"/> set-internal-priority <input type="text"/> <input type="checkbox"/> set-Drop-Precedence <input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

---

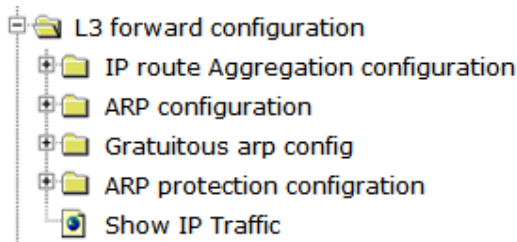
#### 4.16.7 QoS service policy configuration.

Choose **QoS configuration > QoS service policy configuration**, and the following page appears. You can apply the policy-map to a VLAN.

QoS service policy configuration	
Policy-map name	<input type="text"/>
Vlan List	<input type="text"/>
Operation	<input type="text" value="Add"/>
<input type="button" value="Apply"/>	

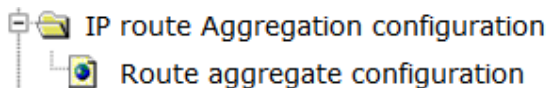
#### 4.17 L3 forward configuration.

Choose **L3 forward configuration**, and the following page appears. There are "IP route Aggregation configuration", "ARP configuration", "Gratuitous ARP config", "ARP protection configuration", "Show IP Traffic", configuration web pages.



##### 4.17.1 IP route Aggregation configuration.

Choose **L3 forward configuration > IP route Aggregation configuration**, and the following page appears. There are "Route aggregate configuration", configuration web pages.



##### 4.17.1.1 Route aggregate configuration.

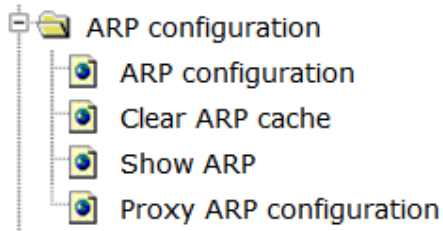
Choose **L3 forward configuration > IP route Aggregation configuration > Route aggregate configuration**, and the following page appears. You can enable or disable the route aggregation function.

Enable route aggregation	
Enable route aggregation	Disable ▾
<input type="button" value="Apply"/>	

Route aggregation status	
Route aggregation status	disable

#### 4.17.2 ARP configuration.

Choose **L3 forward configuration > ARP configuration**, and the following page appears. There are "ARP configuration", "Clear ARP cache", "Show ARP", "Proxy ARP configuration", configuration web pages.



##### 4.17.2.1 ARP configuration.

Choose **L3 forward configuration > ARP configuration > ARP configuration**, and the following page appears. You can add IP, MAC, VLAN and port binding rules.

ARP configuration	
IP address	<input type="text"/>
MAC address	<input type="text"/>
Operation type	Add ▾
VLAN interface	Vlan1 ▾
Port	Ethernet1/0/1 ▾
<input type="button" value="Apply"/>	

##### 4.17.2.2 Clear ARP cache.

Choose **L3 forward configuration > ARP configuration > Clear ARP cache**, and the following page appears. You can clear the ARP cache table.

Clear ARP cache

Information feedback window

```
clear all arp cache
switch# clear arp-cache
```

### 4.17.2.3 Show ARP.

Choose **L3 forward configuration > ARP configuration > Show ARP**, and the following page appears.You can show the ARP list.

ARP list

Binding IP	Binding MAC	Interface	Port	flag
192.168.2.22	c8-be-19-d2-c0-9b	Vlan1	Ethernet1/0/7	dynamic

Number of ARP entry

Number of ARP entry	1
---------------------	---

Refresh

### 4.17.2.4 Proxy ARP configuration.

Choose **L3 forward configuration > ARP configuration > Proxy ARP configuration**, and the following page appears.You can enable or disable the ARP proxy function for each VLAN.

Proxy ARP configuration

Interface

Vlan1 ▾

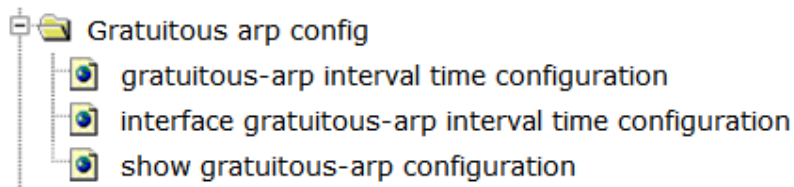
Operation

Enable ▾

Interface	Status
Vlan1	Disable

### 4.17.3 Gratuitous ARP config.

Choose **L3 forward configuration > Gratuitous ARP config**, and the following page appears.There are "Gratuitous-ARP interval time configuration", "Interface Gratuitous-ARP interval time configuration", "Show Gratuitous-ARP configuration", configuration web pages.



#### 4.17.3.1 Gratuitous-ARP interval time configuration.

Choose **L3 forward configuration > Gratuitous ARP config > Gratuitous-ARP interval time configuration**, and the following page appears. You can set up the Gratuitous-ARP interval time.

gratuitous-arp interval time configuration	
interval time	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window	
interval time	300

#### 4.17.3.2 Interface Gratuitous-ARP interval time configuration.

Choose **L3 forward configuration > Gratuitous ARP config > Interface Gratuitous-ARP interval time configuration**, and the following page appears. You can set the gratuitous-arp interval time for each VLAN.

interface gratuitous-arp interval time configuration	
Vlan ID	1 ▾
interval time	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Information feedback window	
Vlan1	300

#### 4.17.3.3 Show Gratuitous-ARP configuration.

Choose **L3 forward configuration > Gratuitous ARP config > Show Gratuitous-ARP configuration**, and the following page appears. You can show the gratuitous-arp information for each VLAN.



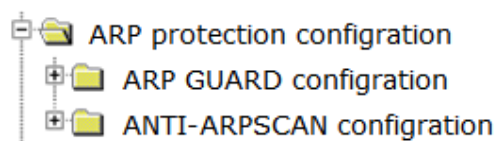
gratuitous-arp interval time configuration	
Vlan ID	<input type="text"/>
<input type="button" value="Apply"/>	

```

Information feedback window
switch# show ip gratuitous-arp interface vlan 1
Gratuitous ARP send interface Vlan1 information:
Name          Interval-Time(seconds)
Gratuitous ARP send disabled
  
```

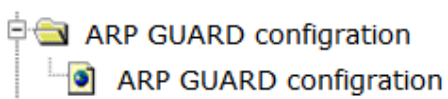
#### 4.17.4 ARP protection configuration.

Choose **L3 forward configuration > ARP protection configuration**, and the following page appears. There are "ARP GUARD configuration", "ANTI-ARPSCAN configuration", configuration web pages.



##### 4.17.4.1 ARP protection configuration.

Choose **L3 forward configuration > ARP protection configuration > ARP protection configuration**, and the following page appears. There are "ARP GUARD configuration", configuration web pages.



##### 4.17.4.1.1 ARP GUARD configuration.

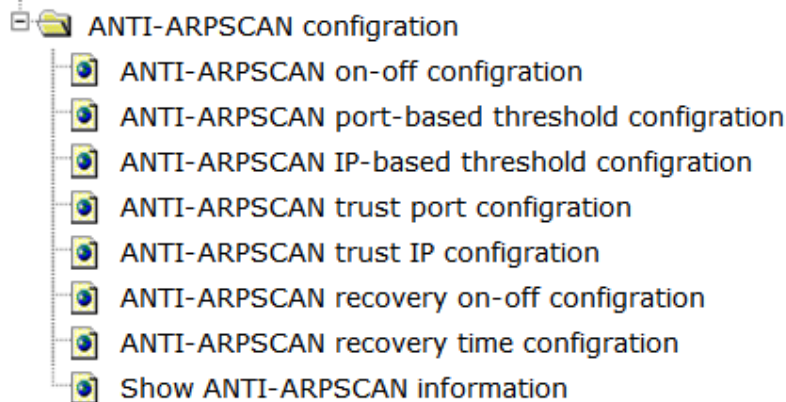
Choose **L3 forward configuration > ARP protection configuration > ARP protection configuration > ARP protection configuration**, and the following page appears. You can configure the arp guard IP address for each port.

ARP GUARD configuration	
Port	<input type="text" value="Ethernet1/0/1"/>
IP address	<input type="text"/>
Operation	<input type="text" value="Add"/>
<input type="button" value="Apply"/>	

---

#### 4.17.4.2 ANTI-ARPSCAN configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration**, and the following page appears. There are "ANTI-ARPSCAN on-off configuration", "ANTI-ARPSCAN port-based threshold configuration", "ANTI-ARPSCAN IP-based threshold", "ANTI-ARPSCAN trust port configuration", "ANTI-ARPSCAN trust IP configuration", "ANTI-ARPSCAN recovery on-off configuration", "ANTI-ARPSCAN recovery time configuration", "Show ANTI-ARPSCAN information", configuration web pages.



##### 4.17.4.2.1 ANTI-ARPSCAN on-off configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN on-off configuration**, and the following page appears. You can enable or disable ANTI-ARPSCAN.

ANTI-ARPSCAN on-off configuration	
ANTI-ARPSCAN on-off status	Disable ▾
<div>Apply</div>	

ANTI-ARPSCAN on-off status	
ANTI-ARPSCAN on-off status	Disable

##### 4.17.4.2.2 ANTI-ARPSCAN port-based threshold configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN port-based threshold configuration**, and the following page appears. You can set the threshold value of receiving ARP message for the port-base anti-arpscan function.

ANTI-ARPSCAN port-based threshold configuration	
Range of threshold	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

ANTI-ARPSCAN port-based threshold configuration	
Range of threshold	10

#### 4.17.4.2.3 ANTI-ARPSCAN IP-based threshold.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN IP-based threshold**, and the following page appears. You can set the threshold value of receiving ARP message for the IP-base anti-arp scan function.

ANTI-ARPSCAN IP-based threshold configuration	
Range of threshold	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

ANTI-ARPSCAN IP-based threshold configuration	
Range of threshold	3

#### 4.17.4.2.4 ANTI-ARPSCAN trust port configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN trust port configuration**, and the following page appears. You can set the trust-port or supertrust-port for anti-arp scan function.

ANTI-ARPSCAN trust port configuration	
Port	Ethernet1/0/1 ▼
Port trust status	trust-port ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.17.4.2.5 ANTI-ARPSCAN trust IP configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN**

---

**configuration > ANTI-ARPSCAN trust IP configuration**, and the following page appears. You can set the trust IP for anti-arpscan function.

ANTI-ARPSCAN trust IP configuration	
IP address	<input type="text"/>
Network mask	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

#### 4.17.4.2.6 ANTI-ARPSCAN recovery on-off configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN recovery on-off configuration**, and the following page appears. You can enable or disable the recovery function for anti-arpscan.

ANTI-ARPSCAN recovery on-off configuration	
ANTI-ARPSCAN recovery on-off status	Enable ▾
<input type="button" value="Apply"/>	

ANTI-ARPSCAN recovery on-off status	
ANTI-ARPSCAN recovery on-off status	Enable

#### 4.17.4.2.7 ANTI-ARPSCAN recovery time configuration.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > ANTI-ARPSCAN recovery time configuration**, and the following page appears. You can set ANTI-ARPSCAN recovery time.

ANTI-ARPSCAN recovery time configuration	
Recovery time	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

ANTI-ARPSCAN recovery time configuration	
Recovery time	300

#### 4.17.4.2.8 Show ANTI-ARPSCAN information.

Choose **L3 forward configuration > ARP protection configuration > ANTI-ARPSCAN configuration > Show ANTI-ARPSCAN information**, and the following page appears. You can show the detail information of the anti-arpscan function.

Information feedback window			
switch# show anti-arpscan			
Total port: 28			
Name	Port-property	beShut	shutTime(seconds)
Ethernet1/0/1	untrust	N	0
Ethernet1/0/2	untrust	N	0
Ethernet1/0/3	untrust	N	0
Ethernet1/0/4	untrust	N	0
Ethernet1/0/5	untrust	N	0
Ethernet1/0/6	untrust	N	0
Ethernet1/0/7	untrust	N	0
Ethernet1/0/8	untrust	N	0
Ethernet1/0/9	untrust	N	0
Ethernet1/0/10	untrust	N	0
Ethernet1/0/11	untrust	N	0
Ethernet1/0/12	untrust	N	0
Ethernet1/0/13	untrust	N	0
Ethernet1/0/14	untrust	N	0
Ethernet1/0/15	untrust	N	0
Ethernet1/0/16	untrust	N	0
Ethernet1/0/17	untrust	N	0
Ethernet1/0/18	untrust	N	0
Ethernet1/0/19	untrust	N	0
Ethernet1/0/20	untrust	N	0
Ethernet1/0/21	untrust	N	0
Ethernet1/0/22	untrust	N	0
Ethernet1/0/23	untrust	N	0
Ethernet1/0/24	untrust	N	0
Ethernet1/0/25	untrust	N	0
Ethernet1/0/26	untrust	N	0
Ethernet1/0/27	untrust	N	0
Ethernet1/0/28	untrust	N	0
No prohibited IP.			
No configured trust IP.			

#### 4.17.5 Show IP Traffic.

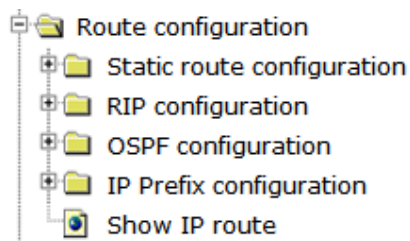
Choose **L3 forward configuration**, and the following page appears. You can show the statistics for different traffic protocol.

#### Information feedback window

```
switch# show ip traffic
IP statistics:
  Rcvd: 98575 total, 99466 local destination
        0 header errors, 0 address errors
        0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
        0 fragment rcvd, 0 fragment dropped
        0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent: 128480 generated, 0 forwarded
        2 dropped, 0 no route
ICMP statistics:
  Rcvd: 0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
  Sent: 0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens      83, TcpAttemptFails      0
  TcpCurrEstab        3, TcpEstabResets        131
  TcpInErrs           0, TcpInSegs            99463
  TcpMaxConn          768, TcpOutRsts           0
  TcpOutSegs          129366, TcpPassiveOpens    13809
  TcpRetransSegs       0, TcpRtoAlgorithm       1
  TcpRtoMax           120000, TcpRtoMin         200
UDP statistics:
  UdpInDatagrams      0, UdpInErrors        0
  UdpNoPorts          0, UdpOutDatagrams      3
```

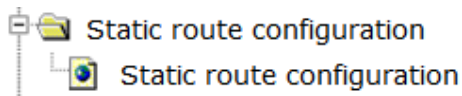
## 4.18 Route configuration.

Choose **Route configuration**, and the following page appears. There are "Static route configuration", "RIP configuration", "OSPF configuration", "IP Prefix configuration", "Show IP route", configuration web pages.



### 4.18.1 Static route configuration.

Choose **Route configuration > Static route configuration**, and the following page appears.



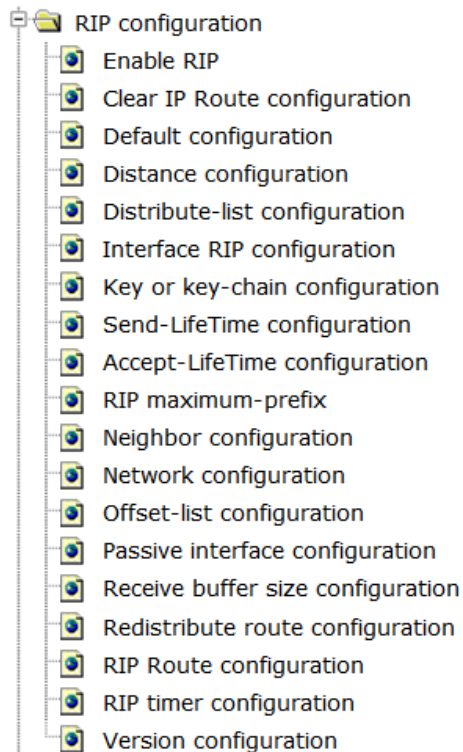
#### 4.18.1.1 Static route configuration.

Choose **Route configuration > Static route configuration**, and the following page appears. You can configure static IP route rules to indicate the route arrive to the destination IP.

Static IP route configuration	
Destination IP address	<input type="text"/>
Network mask or prefix-length	<input type="text"/>
Nexthop or Interface null0	<input type="text"/>
preference(optional)	<input type="text"/>
Operation type	Add <input type="button" value="▼"/>
<input type="button" value="Apply"/>	

#### 4.18.2 RIP configuration.

Choose **Route configuration > RIP configuration**, and the following page appears. There are "Enable RIP", "Clear IP Route configuration", "Default configuration", "Distance configuration", "Distribute-list configuration", "Interface RIP configuration", "Key or key-chain configuration", "Send-LifeTime configuration", "Accept-LiftTime configuration", "RIP maximum-prefix", "Neighbor configuration", "Network configuration", "Offset-list configuration", "Passive interface configuration", "Receive buffer size configuration", "Receive route configuration", "RIP route configuration", "RIP timer configuration", "Version configuration", configuration web pages.



#### 4.18.2.1 Enable RIP.

Choose **Route configuration > RIP configuration > Enable RIP**, and the following page appears. You can enable or disable the RIP function.

Enable RIP configuration	
Enable RIP	Enable ▾
<div>Apply</div>	

#### 4.18.2.2 Clear IP Route configuration.

Choose **Route configuration > RIP configuration > Clear IP Route configuration**, and the following page appears. You can clear the IP route by different classes, the route class include IP-address, kernel, static, connected, rip, OSPF, ISIS, BGP, ALL.

Clear IP Route configuration	
Route class	ip-address ▾
IP address(A.B.C.D/M)	<input type="text"/>
<div>Apply</div>	



---

#### 4.18.2.3 Default configuration.

Choose **Route configuration > RIP configuration > Default configuration**, and the following page appears. You can originate the default-information to RIP. And set the default-metric value.

Default-information configuration	
Operation	Add ▼
<div>Apply</div>	

---

Default-metric configuration	
Default-metric	<input type="text"/>
Operation	Add ▼
<div>Apply</div>	

#### 4.18.2.4 Distance configuration.

Choose **Route configuration > RIP configuration > Distance configuration**, and the following page appears. You can set the distance for IP segment, and set the access-list.

Distance configuration	
Distance	<input type="text"/>
IP address(Optional)	<input type="text"/>
Access-list name(Optional)	<input type="text"/>
Operation	Configuration ▼
<div>Apply</div>	

#### 4.18.2.5 Distribute-list configuration.

Choose **Route configuration > RIP configuration > Distribute-list configuration**, and the following page appears. You can set the distribute-list, the filter method can be by prefix-list or access-list, the filter mode can be out or in.

Distribute-list configuration	
Prefix-list or access-list	access-list name ▾
Prefix-list or access-list name	<input type="text"/>
Filter mode	out ▾
Interface name	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

#### 4.18.2.6 Interface RIP configuration.

Choose **Route configuration > RIP configuration > Interface RIP configuration**, and the following page appears. You can configure the RIP interface via different command include ip rip authentication key-chain, ip rip authentication mode, ip rip authentication string, ip rip authentication cisco-compatible, no ip rip receive-packet, ip rip receive version, no ip rip send-packet, ip rip send version, ip rip split-horizon.

Interface RIP configuration	
Command	ip rip authentication key-chain ▾
VLAN interface	Vlan1 ▾
Key chain	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.18.2.7 Key or key-chain configuration.

Choose **Route configuration > RIP configuration > Key or key-chain configuration**, and the following page appears. You can set Key chain, key and key string parameters.

Key chain management	
Key chain	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Key management	
Key chain	<input type="text"/>
Key ID	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

Key string management	
Key chain	<input type="text"/>
Key ID	<input type="text"/>
Key string	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

---

#### 4.18.2.8 Send-LifeTime configuration.

Choose **Route configuration > RIP configuration > Send-LifeTime configuration**, and the following page appears. You can set Send-Lift time parameters include end-time, duration, infinite.

Send-LifeTime configuration	
Parameter choose	end-time ▼
Key chain	<input type="text"/>
Key ID	<input type="text"/>
HH:MM:SS	<input type="text"/>
Month	<input type="text"/>
Day	<input type="text"/>
Year	<input type="text"/>
HH:MM:SS	<input type="text"/>
Month	<input type="text"/>
Day	<input type="text"/>
Year	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.2.9 Accept-LiftTime configuration.

Choose **Route configuration > RIP configuration > Accept-LiftTime configuration**, and the following page appears. You can set Accept-Lift time parameters include end-time, duration, infinite.

Accept-LifeTime configuration	
Parameter choose	end-time ▼
Key chain	<input type="text"/>
Key ID	<input type="text"/>
HH:MM:SS	<input type="text"/>
Month	<input type="text"/>
Day	<input type="text"/>
Year	<input type="text"/>
HH:MM:SS	<input type="text"/>
Month	<input type="text"/>
Day	<input type="text"/>
Year	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

---

#### 4.18.2.10 RIP maximum-prefix.

Choose **Route configuration > RIP configuration > RIP maximum-prefix**, and the following page appears. You can configure the RIP maximum-prefix.

RIP maximum-prefix	
Prefix number	<input type="text"/>
Threshold(Optional)	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.18.2.11 Neighbor configuration.

Choose **Route configuration > RIP configuration > Neighbor configuration**, and the following page appears. You can set the IP address of the neighbor.

Neighbor configuration	
Neighbor address	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

#### 4.18.2.12 Network configuration.

Choose **Route configuration > RIP configuration > Network configuration**, and the following page appears. You can set the network section that allow to notice RIP.

Network configuration	
Notice network section	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

#### 4.18.2.13 Offset-list configuration.

Choose **Route configuration > RIP configuration > Offset-list configuration**, and the following page appears. You can set the offset-list to add the metric for route.

---

Offset-list configuration	
List name	<input type="text"/>
Offset operate	in ▼
Additional offset	<input type="text"/>
Interface operate	Add ▼
Interface name	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.2.14 Passive interface configuration.

Choose **Route configuration > RIP configuration > Passive interface configuration**, and the following page appears. You can set the passive interface.

Passive interface configuration	
Interface name	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.2.15 Receive buffer size configuration.

Choose **Route configuration > RIP configuration > Receive buffer size configuration**, and the following page appears. You can configure the receive buffer size.

Receive buffer size configuration	
Receive buffer size	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

#### 4.18.2.16 Receive route configuration.

Choose **Route configuration > RIP configuration > Receive route configuration**, and the following page appears. You can set the redistribute route rule, the offset operate include kernel, connected, static, ospf, isis, bgp.

Redistribute route configuration	
Offset operate	kernel ▼
Redistribute route metric value(Optional)	<input type="text"/>
Redistribute route-map(Optional)	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.2.17 RIP route configuration.

Choose **Route configuration > RIP configuration > RIP route configuration**, and the following page appears. You can add or remove RIP Route.

RIP Route configuration	
IP address and prefix length	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.2.18 RIP timer configuration.

Choose **Route configuration > RIP configuration > RIP timer configuration**, and the following page appears. You can set the timers for RIP.

RIP timer configuration	
Update time	<input type="text"/>
Invalid time	<input type="text"/>
Garbage time	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

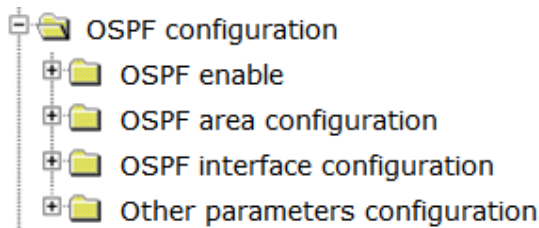
#### 4.18.2.19 Version configuration.

Choose **Route configuration > RIP configuration > Version configuration**, and the following page appears. You can configure the version to RIP1 or RIP2.

Version configuration	
Version	1 ▼
Operation	Configuration ▼
<input type="button" value="Apply"/>	

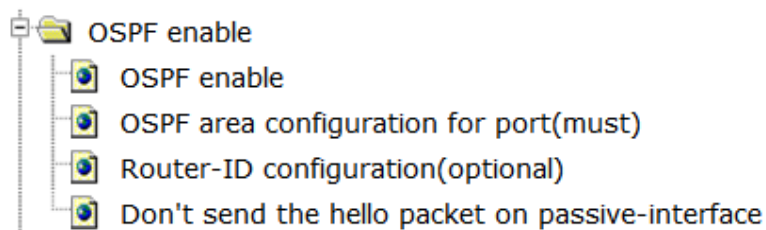
### 4.18.3 OSPF configuration.

Choose **Route configuration > OSPF configuration**, and the following page appears. There are "OSPF enable", "OSPF area configuration", "OSPF interface configuration", "Other parameters configuration", configuration web pages.



#### 4.18.3.1 OSPF enable.

Choose **Route configuration > OSPF configuration > OSPF enable**, and the following page appears. There are "OSPF enable", "OSPF area configuration for port(must)", "Router-ID configuration(optional)", "Don't send the hello packet on passive-interface", configuration web pages.



##### 4.18.3.1.1 OSPF enable.

Choose **Route configuration > OSPF configuration > OSPF enable > OSPF enable**, and the following page appears. You can enable or disable OSPF function.

OSPF enable	
Process ID	<input type="text"/>
OSPF enable	Open ▼
<input type="button" value="Apply"/>	

##### 4.18.3.1.2 OSPF area configuration for port(must).

Choose **Route configuration > OSPF configuration > OSPF enable > OSPF area configuration for port(must)**, and the following page appears. You can configure OSPF

areas.

OSPF area configuration for port(must)	
Process ID	<input type="text"/>
Network address	<input type="text"/>
Network mask or prefix-length	<input type="text"/>
Area Number	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.3.1.3 Router-ID configuration(optional).

Choose **Route configuration > OSPF configuration > OSPF enable > Router-ID configuration(optional)**, and the following page appears.You can configure the router-ID for the OSPF process.

Router-ID configuration(optional)	
Process ID	<input type="text"/>
Router ID	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.3.1.4 Don't send the hello packet on passive-interface.

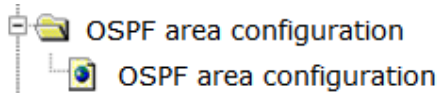
Choose **Route configuration > OSPF configuration > OSPF enable > Don't send the hello packet on passive-interface**, and the following page appears.You can set the passive-interfaces don't send hello packet anymore.

Don't send the hello packet on passive-interface	
Process ID	<input type="text"/>
Interface	<input type="text"/>
IP address	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.3.2 OSPF area configuration.

Choose **Route configuration > OSPF configuration > OSPF area configuration**, and the following page appears.There are "OSPF area configuration", configuration web pages.





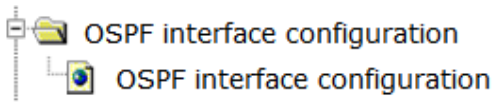
#### 4.18.3.2.1 OSPF area configuration.

Choose **Route configuration > OSPF configuration > OSPF area configuration > OSPF area configuration**, and the following page appears. You can set different parameters for OSPF area, the operation type include authentication, default-cost, filter-list, nssa, range, stub, virtual-link.

OSPF area configuration	
Operation type	authentication ▼
Process ID	<input type="text"/>
Area Number	<input type="text"/>
OSPF area authentication	
Auth type	Message-digest (MD5) ▼
Operation type	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.3.3 OSPF interface configuration.

Choose **Route configuration > OSPF configuration > OSPF interface configuration**, and the following page appears. There are "OSPF interface configuration", configuration web pages.



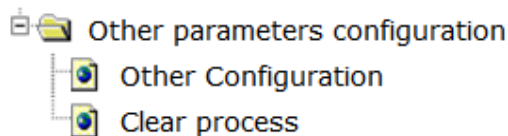
#### 4.18.3.3.1 OSPF interface configuration.

Choose **Route configuration > OSPF configuration > OSPF interface configuration > OSPF interface configuration**, and the following page appears. You can set different parameters for OSPF interface, the operation type include authentication, authentication-key, cost, database-filter, dead-interval, disable, hello-interval, message-digest-key, mtu, mtu-ignore, network, priority, retransmit-interval, transmit-delay.

OSPF interface configuration	
Operation type	authentication ▼
VLAN interface	1 ▼
Enable authentication on interface	
Interface address	<input type="text"/>
Auth type	null ▼
Operation type	Add ▼
<input type="button" value="Apply"/>	

#### 4.18.3.4 Other parameters configuration.

Choose **Route configuration > OSPF configuration > Other parameters configuration**, and the following page appears. There are "Other Configuration", "Clear process", configuration web pages.



##### 4.18.3.4.1 Other Configuration.

Choose **Route configuration > OSPF configuration > Other parameters configuration > Other Configuration**, and the following page appears. You can set other parameters for OSPF, the operation type include auto-cost, compatible, default-information, default-metric, distance, distribute-list, host, max-concurrent-dd, neighbor, abr-type, database, database-external, passive-interface, redistribute, summary-address, timers-spf.

Other Configuration	
Operation type	auto-cost ▼
Process ID	<input type="text"/>
Calculate OSPF interface cost according to bandwidth	
Bandwidth	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

##### 4.18.3.4.2 Clear process.

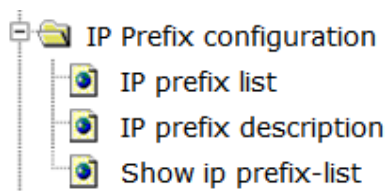
Choose **Route configuration > OSPF configuration > Other parameters configuration > Clear process**, and the following page appears. You can clear OSPF process.

---

Clear process	
Process ID	<input type="text"/>
<input type="button" value="Apply"/>	

#### 4.18.4 IP Prefix configuration.

Choose **Route configuration > IP Prefix configuration**, and the following page appears. There are "IP prefix list", "IP prefix description", "Show IP prefix-list", configuration web pages.



##### 4.18.4.1 IP prefix list.

Choose **Route configuration > IP Prefix configuration > IP prefix list**, and the following page appears. You can set IP prefix list to deny or permit designated IP section accessing.

IP prefix list	
IP prefix name	<input type="text"/>
IP prefix num	<input type="text"/>
Mode	deny ▼
IP prefix address	any ▼
IP prefix address/Mask address	<input type="text"/>
MinIP prefix len(ge, Optional)	<input type="text"/>
MaxIP prefix len(le, Optional)	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

##### 4.18.4.2 IP prefix description.

Choose **Route configuration > IP Prefix configuration > IP prefix description**, and the following page appears. You can set description for IP prefix name.

IP prefix description	
IP prefix name	<input type="text"/>
Description	<input type="text"/>
Operation type	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

#### 4.18.4.3 Show IP prefix-list.

Choose **Route configuration > IP Prefix configuration > Show IP prefix-list**, and the following page appears. You can show the IP prefix-list.

Information feedback window
switch# show ip prefix-list

#### 4.18.5 Show IP route.

Choose **Route configuration > Show IP route**, and the following page appears. You can show IP route with different parameter include destination, prefix, database, connected, static, rip, ospf, bgp, isis, kernel, statistics.

Show IP route	
Parameter choose	<input type="text"/>
<input type="button" value="Apply"/>	

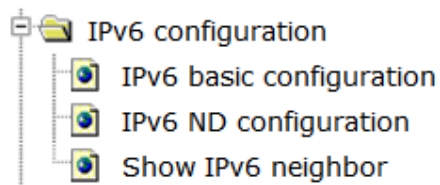
### 4.19 IPv6 Route configuration.

Choose **IPv6 Route configuration**, and the following page appears. There are "IPv6 configuration", "Show IPv6 route", configuration web pages.

- ☐ IPv6 Route configuration
  - ☐ IPv6 configuration
  - ☐ Show IPv6 route

#### 4.19.1 IPv6 configuration.

Choose **IPv6 Route configuration > IPv6 configuration**, and the following page appears. There are "IPv6 basic configuration", "IPv6 ND configuration", "Show IPv6 neighbor", configuration web pages.



#### 4.19.1.1 IPv6 basic configuration.

Choose **IPv6 Route configuration > IPv6 configuration > IPv6 basic configuration**, and the following page appears. You can set the IPv6 address or IPv6 route for VLAN.

IPv6 basic configuration	
command	ipv6 address ▾
VLAN interface	Vlan1 ▾
IPv6 address(X:X::X:X/M)	<input type="text"/>
EUI-64	▾
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.19.1.2 IPv6 ND configuration.

Choose **IPv6 Route configuration > IPv6 configuration > IPv6 ND configuration**, and the following page appears. You set IPv6 ND parameters via different command include dad attempts, ns-interval, supress-ra, ra-lifetime, min-ra-interval, max-ra-interval, prefix, neighbor, clear ipv6 neighbor.

IPv6 ND configuration	
command	dad attempts ▾
VLAN interface	Vlan1 ▾
IPv6 dad-attempts	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.19.1.3 Show IPv6 neighbor.

Choose **IPv6 Route configuration > IPv6 configuration > Show IPv6 neighbor**, and the following page appears. You can show IPv6 neighbor by Address, Count, VLAN, Ethernet.

---

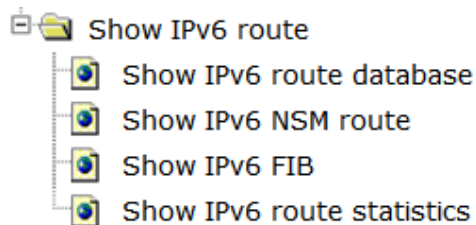
Show IPv6 neighbor

Parameter choose

Apply

#### 4.19.2 Show IPv6 route.

Choose **IPv6 Route configuration > Show IPv6 route**, and the following page appears. There are "Show IPv6 route database", "Show IPv6 NSM route", "Show IPv6 FIB", "Show IPv6 route statistics", configuration web pages.



##### 4.19.2.1 Show IPv6 route database.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 route database**, and the following page appears. You can show IPv6 route database by destination, prefix, database.

Show IPv6 route database

Parameter choose

Apply

##### 4.19.2.2 Show IPv6 NSM route.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 NSM route**, and the following page appears. You can show IPv6 NSM route by parameter include static, bgp, isis, rip, ospf, connected, kernel, database.

Show IPv6 NSM route

Parameter choose 

static

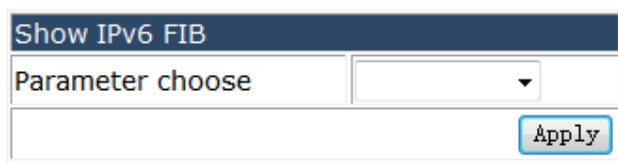
Apply

##### 4.19.2.3 Show IPv6 FIB.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 FIB**, and the

---

following page appears. You can show IPv6 FIB by local, vrf, statistics.



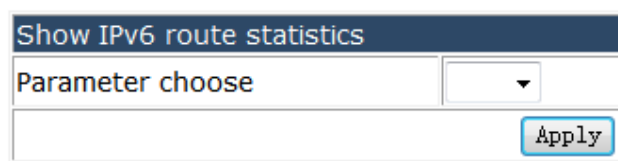
Show IPv6 FIB

Parameter choose ▼

Apply

#### 4.19.2.4 Show IPv6 route statistics.

Choose **IPv6 Route configuration > Show IPv6 route > Show IPv6 route statistics**, and the following page appears. You can show IPv6 statistics by vrf.



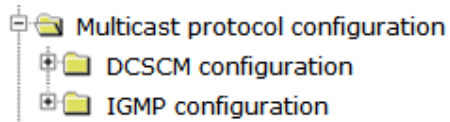
Show IPv6 route statistics

Parameter choose ▼

Apply

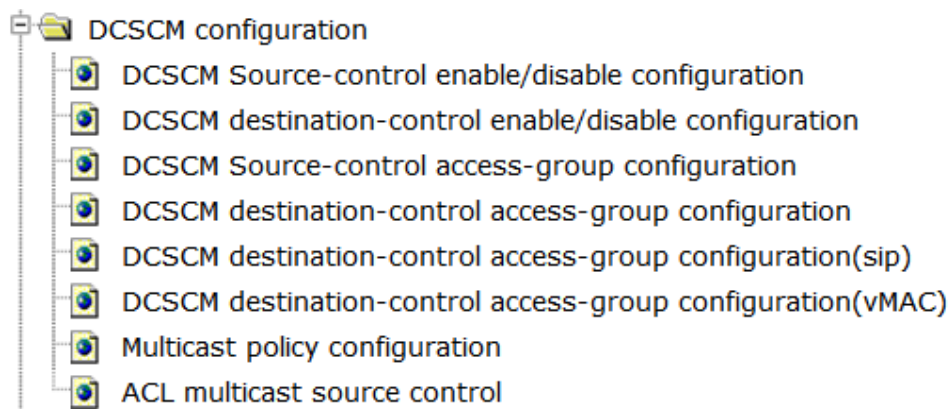
### 4.20 Multicast protocol configuration.

Choose **Multicast protocol configuration**, and the following page appears. There are "DCSCM configuration", "IGMP configuration", configuration web pages.



#### 4.20.1 DCSCM configuration.

Choose **Multicast protocol configuration > DCSCM configuration**, and the following page appears. There are "DCSCM Source-control enable/disable configuration", "DCSCM destination-control enable/disable configuration", "DCSCM Source-control access-group configuration", "DCSCM destination-control access-group configuration", "DCSCM destination-control access-group configuration(SIP)", "DCSCM destination-control access-group configuration(vMAC)", "Multicast policy configuration", "ACL multicast source control", configuration web pages.



#### 4.20.1.1 DCSCM Source-control enable/disable configuration.

Choose **Multicast protocol configuration > DCSCM configuration > DCSCM Source-control enable/disable configuration**, and the following page appears. You can Enable or Disable DCSCM Source-control.

DCSCM Source-control enable/disable configuration	
DCSCM Source-control enable/disable configuration	Enable ▾
<input type="button" value="Apply"/>	

DCSCM Source-control state	
DCSCM Source-control state	Enable

#### 4.20.1.2 DCSCM destination-control enable/disable configuration.

Choose **Multicast protocol configuration > DCSCM configuration > DCSCM destination-control enable/disable configuration**, and the following page appears. You can Enable or Disable DCSCM destination-control.

DCSCM destination-control enable/disable configuration	
DCSCM destination-control enable/disable configuration	Enable ▾
<input type="button" value="Apply"/>	

DCSCM destination-control enable/disable state	
DCSCM destination-control enable/disable state	Enable



---

#### 4.20.1.3 DCSCM Source-control access-group configuration.

Choose **Multicast protocol configuration > DCSCM configuration > DCSCM Source-control access-group configuration**, and the following page appears. You can add or remove DCSCM Source-control access-group.

DCSCM Source-control access-group configuration	
Port	Ethernet1/0/1 ▾
DCSCM Source-control access-group number	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

DCSCM Source-control access-group	
Port	DCSCM Source-control access-group number

#### 4.20.1.4 DCSCM destination-control access-group configuration.

Choose **Multicast protocol configuration > DCSCM configuration > DCSCM Source-control access-group configuration**, and the following page appears. You can add or remove DCSCM destination-control access-group.

DCSCM destination-control access-group configuration	
Port	Ethernet1/0/1 ▾
DCSCM destination-control access-group number	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

DCSCM destination-control access-group	
Port	DCSCM destination-control access-group number

#### 4.20.1.5 DCSCM destination-control access-group configuration(SIP).

Choose **Multicast protocol configuration > DCSCM configuration > DCSCM Source-control access-group configuration(SIP)**, and the following page appears. You can add or remove DCSCM destination-control access-group(SIP).

DCSCM destination-control access-group configuration(sip)	
DCSCM destination-control IP-address/mask	<input type="text"/>
DCSCM destination-control access-group number	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

DCSCM destination-control access-group(sip)	
DCSCM destination-control IP-address/mask	DCSCM destination-control access-group number

#### 4.20.1.6 DCSCM destination-control access-group configuration(vMAC).

Choose **Multicast protocol configuration > DCSCM configuration > DCSCM Source-control access-group configuration(vMAC)**, and the following page appears. You can add or remove DCSCM Source-control access-group(vMAC).

DCSCM destination-control access-group configuration(vMAC)	
VLAN interface	Vlan1 ▼
MAC address	<input type="text"/>
DCSCM destination-control access-group number	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

DCSCM destination-control access-group(vMAC)		
VLAN interface	MAC address	DCSCM destination-control access-group number

#### 4.20.1.7 Multicast policy configuration.

Choose **Multicast protocol configuration > DCSCM configuration > Multicast policy configuration**, and the following page appears. You can set the DCSCM multicast policy.

Multicast policy configuration	
Source IP-address/mask	<input type="text"/>
Destination IP-address/mask	<input type="text"/>
DCSCM priority	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

Multicast policy
------------------

#### 4.20.1.8 ACL multicast source control.

Choose **Multicast protocol configuration > DCSCM configuration > ACL multicast source control**, and the following page appears. You can set the ACL multicast source and

destination control to permit or deny the designated IP address.

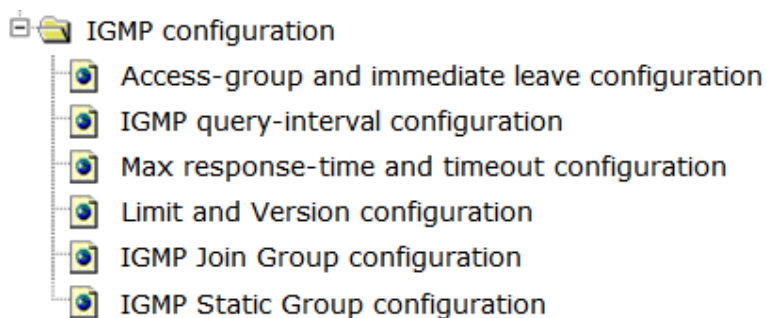
ACL multicast source control	
ACL number	<input type="text"/>
Rule	permit ▼
Source address type	Any IP ▼
Multicast source address	<input type="text"/>
Multicast source wildcard	<input type="text"/>
Source address type	Any IP ▼
Multicast destination address	<input type="text"/>
Multicast destination wildcard	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

ACL multicast destination control	
ACL number	<input type="text"/>
Rule	permit ▼
Source address type	Any IP ▼
Multicast source address	<input type="text"/>
Multicast source wildcard	<input type="text"/>
Source address type	Any IP ▼
Multicast destination address	<input type="text"/>
Multicast destination wildcard	<input type="text"/>
Operation type	Add ▼
<input type="button" value="Apply"/>	

```
Information feedback window
switch# show ip multicast source-control access-list
switch# show ip multicast destination-control access-list
```

#### 4.20.2 IGMP configuration.

Choose **Multicast protocol configuration > IGMP configuration**, and the following page appears. There are "Access-group and immediate leave configuration", "IGMP query-interval configuration", "Max response-time and timeout configuration", "Limit and Version configuration", "IGMP Join Group configuration", "IGMP Static Group configuration", configuration web pages.



##### 4.20.2.1 Access-group and immediate leave configuration.

Choose **Multicast protocol configuration > IGMP configuration > Access-group and immediate leave configuration**, and the following page appears. You can set the IGMP access-group and immediate-leave group for VLAN.

---

Access-group configuration	
VLAN interface	Vlan1 ▾
Access-num	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Immediate-leave configuration	
VLAN interface	Vlan1 ▾
Ad-list num	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.20.2.2 IGMP query-interval configuration.

Choose **Multicast protocol configuration > IGMP configuration > IGMP query-interval configuration**, and the following page appears. You can set the IGMP query-interval and last-member-query-interval for VLAN.

IGMP query-interval configuration	
VLAN interface	Vlan1 ▾
IGMP query-interval	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

IGMP last-member-query-interval configuration	
VLAN interface	Vlan1 ▾
IGMP last-member-query-interval	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.20.2.3 Max response-time and timeout configuration.

Choose **Multicast protocol configuration > IGMP configuration > Max response-time and timeout configuration**, and the following page appears. You can set the query timeout value and query-max-response-time for VLAN.

---

Query timeout configuration	
VLAN interface	Vlan1 ▾
Query timeout	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Query-max-response-time configuration	
VLAN interface	Vlan1 ▾
Query-max-response-time	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.20.2.4 Limit and Version configuration.

Choose **Multicast protocol configuration > IGMP configuration > Limit and Version configuration**, and the following page appears. You can set the IGMP version and limit parameter.

Version configuration	
VLAN interface	Vlan1 ▾
Version	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Limit configuration	
VLAN interface	Vlan1 ▾
Limit	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.20.2.5 IGMP Join Group configuration.

Choose **Multicast protocol configuration > IGMP configuration > IGMP Join Group configuration**, and the following page appears. You can add or remove VLAN to a IGMP group.

IGMP Join Group configuration	
VLAN interface	Vlan1 ▾
Group address(A.B.C.D)	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

---

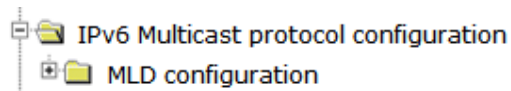
#### 4.20.2.6 IGMP Static Group configuration.

Choose **Multicast protocol configuration > IGMP configuration > IGMP Static Group configuration**, and the following page appears. You can add or remove VLAN to a static IGMP group with designated source.

IGMP Static Group configuration	
VLAN interface	Vlan1 ▾
Group address(A.B.C.D)	<input type="text"/>
SSM address(A.B.C.D)	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

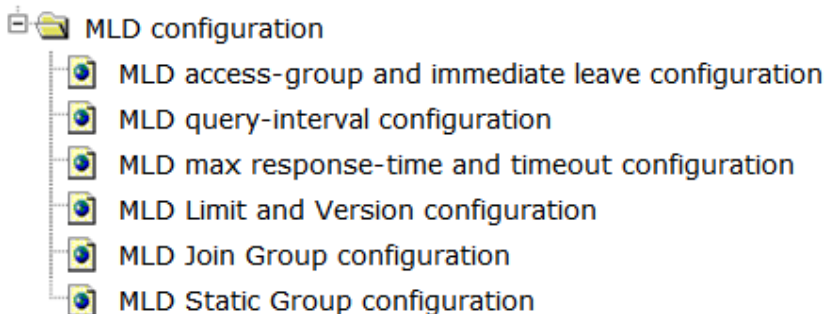
#### 4.21 IPv6 Multicast protocol configuration.

Choose **IPv6 Multicast protocol configuration**, and the following page appears.



##### 4.21.1 MLD configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration**, and the following page appears. There are "MLD access-group and immediate leave configuration", "MLD query-interval configuration", "MLD max response-time and timeout configuration", "MLD Limit and Version configuration", "MLD Join Group configuration", "MLD Static Group configuration", configuration web pages.



##### 4.21.1.1 MLD access-group and immediate leave configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD access-group and immediate leave configuration**, and the following page appears. You can set the IPv6 access-group and IPv6 immediate-leave group for VLAN.

---

Access-group configuration	
VLAN interface	Vlan1 ▾
IPv6 access-name	
Operation	Configuration ▾
<div>Apply</div>	

Immediate-leave configuration	
VLAN interface	Vlan1 ▾
IPv6 ACL-list name	
Operation	Configuration ▾
<div>Apply</div>	

#### 4.21.1.2 MLD query-interval configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD query-interval configuration**, and the following page appears. You can set the MLD query-interval and IGMP last-member-query-interval for VLAN.

MLD query-interval configuration	
VLAN interface	Vlan1 ▾
MLD query-interval	
Operation	Configuration ▾
<div>Apply</div>	

IGMP last-member-query-interval configuration	
VLAN interface	Vlan1 ▾
IGMP last-member-query-interval	
Operation	Configuration ▾
<div>Apply</div>	

#### 4.21.1.3 MLD max response-time and timeout configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD max response-time and timeout configuration**, and the following page appears. You can set the query timeout value and query-max-response-time for VLAN.

---

Query timeout configuration	
VLAN interface	Vlan1 ▾
Query timeout	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Query-max-response-time configuration	
VLAN interface	Vlan1 ▾
Query-max-response-time	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.21.1.4 MLD Limit and Version configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD Limit and Version configuration**, and the following page appears. You can set the MLD version and limit parameter.

Version configuration	
VLAN interface	Vlan1 ▾
Version	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

Limit configuration	
VLAN interface	Vlan1 ▾
Limit	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.21.1.5 MLD Join Group configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD Join Group configuration**, and the following page appears. You can add or remove VLAN to a MLD group and choose to include or exclude designated source.



MLD Join Group configuration	
VLAN interface	Vlan1 ▾
Group address(X:X::X:X)	<input type="text"/>
Source add mode	▾
source address(X:X::X:X)	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

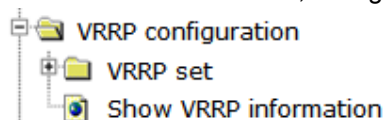
#### 4.21.1.6 MLD Static Group configuration.

Choose **IPv6 Multicast protocol configuration > MLD configuration > MLD Static Group configuration**, and the following page appears. You can add or remove VLAN to a static MLD group with designated source.

MLD Static Group configuration	
VLAN interface	Vlan1 ▾
Group address(X:X::X:X)	<input type="text"/>
Source address(X:X::X:X)	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

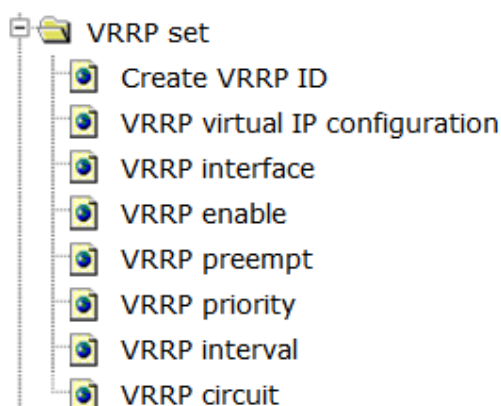
### 4.22 VRRP configuration.

Choose **VRRP configuration**, and the following page appears. There are "VRRP set", "Show VRRP information", configuration web pages.



#### 4.22.1 VRRP set.

Choose **VRRP configuration > VRRP set**, and the following page appears. There are "Create VRRP ID", "VRRP virtual IP configuration", "VRRP interface", "VRRP enable", "VRRP preempt", "VRRP priority", "VRRP interval", "VRRP circuit", configuration web pages.



#### 4.22.1.1 Create VRRP ID.

Choose **VRRP configuration > VRRP set > Create VRRP ID**, and the following page appears. You can create a VRRP ID.

Create VRRP ID	
Create VRRP ID	<input type="text"/>
Operation	Add ▼
<div>Apply</div>	

#### 4.22.1.2 VRRP virtual IP configuration.

Choose **VRRP configuration > VRRP set > VRRP virtual IP configuration**, and the following page appears. You can set the VRRP virtual IP for the VRRP ID.

VRRP virtual IP configuration	
Choose vrid	<input type="text"/>
VRRP virtual IP configuration	<input type="text"/>
Operation	Add ▼
<div>Apply</div>	

#### 4.22.1.3 VRRP interface.

Choose **VRRP configuration > VRRP set > VRRP interface**, and the following page appears. You can set the VLAN interface for the VRRP ID.

---

VRRP interface	
Choose vrid	<input type="text"/>
VLAN interface	Vlan1 ▾
Operation	Add ▾
<div>Apply</div>	

#### 4.22.1.4 VRRP enable.

Choose **VRRP configuration > VRRP set > VRRP enable**, and the following page appears. You can enable or disable the VRRP function for the VRRP ID.

**Notice:** Before enable VRRP, please finish the setting of Virtual IP and Interface

VRRP enable	
Choose vrid	<input type="text"/>
Operation	Enable ▾
<div>Apply</div>	

#### 4.22.1.5 VRRP preempt.

Choose **VRRP configuration > VRRP set > VRRP preempt**, and the following page appears. You can set the VRRP preempt to true or false for VRRP ID.

VRRP preempt	
Choose vrid	<input type="text"/>
VRRP preempt	True ▾
<div>Apply</div>	

#### 4.22.1.6 VRRP priority.

Choose **VRRP configuration > VRRP set > VRRP priority**, and the following page appears.

You can set VRRP Priority.

VRRP priority	
Choose vrid	<input type="text"/>
Priority	<input type="text"/>
<input type="button" value="Apply"/>	

#### 4.22.1.7 VRRP interval.

Choose **VRRP configuration > VRRP set > VRRP interval**, and the following page appears. You can set VRRP interval.

VRRP interval	
Choose vrid	<input type="text"/>
Interval time	<input type="text"/>
<input type="button" value="Apply"/>	

#### 4.22.1.8 VRRP circuit.

Choose **VRRP configuration > VRRP set > VRRP circuit**, and the following page appears. You can set the priority decrease number for the VRRP ID.

VRRP circuit	
Choose vrid	<input type="text"/>
VLAN interface	Vlan1 ▾
Priority decrease number	<input type="text"/>
Operation	Enable ▾
<input type="button" value="Apply"/>	

#### 4.22.2 Show VRRP information.

Choose **VRRP configuration > Show VRRP information**, and the following page appears. You can show the VRRP information.

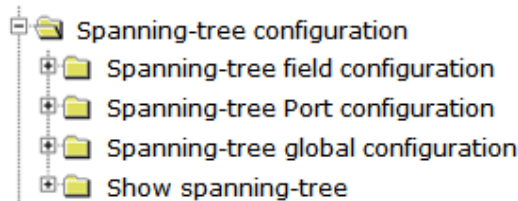
Show VRRP information	
<input type="button" value="Refresh"/>	

Information feedback window
<pre>switch# show vrrp VRRP is not enabled</pre>

---

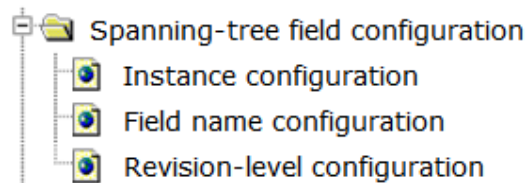
## 4.23 Spanning- tree configuration.

Choose **Spanning- tree configuration**, and the following page appears. There are "Spanning-tree field configuration", "Spanning-tree Port configuration", "Spanning-tree global configuration", "Show Spanning-tree", configuration web pages.



### 4.23.1 Spanning-tree field configuration.

Choose **Spanning- tree configuration > Spanning-tree field configuration**, and the following page appears. There are "Instance configuration", "Field name configuration", "Revision-level configuration", configuration web pages.



#### 4.23.1.1 Instance configuration.

Choose **Spanning- tree configuration > Spanning-tree field configuration > Instance configuration**, and the following page appears. You can configure instance and associate with VLAN.

Instance configuration	
Instance name	<input type="text"/>
VLAN name	<input type="text"/>
Operation	Add <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Instance configuration	
Instance name	VLAN name
0	1-4094

<b>TIPS</b>
When instance configured , the port will be block, and then turn to forwarding; the web will be time-out, please relogin

#### 4.23.1.2 Field name configuration.

Choose **Spanning- tree configuration > Spanning-tree field configuration > Field**

**name configuration**, and the following page appears. You can configure the MSTP field name.

Field name configuration	
Field name	<input type="text"/>
Operation	Configuration ▼
<input type="button" value="Apply"/>	

Field name
<input type="text"/>

#### 4.23.1.3 Revision-level configuration.

Choose **Spanning- tree configuration > Spanning-tree field configuration > Revision-level configuration**, and the following page appears. You can configure MSTP revision-level.

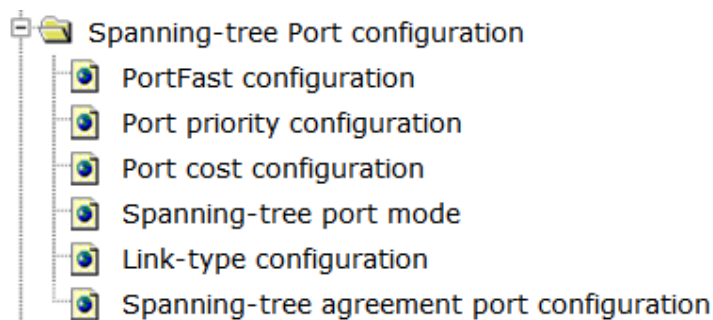
Revision-level configuration	
Revision-level	<input type="text"/>
Operation	Default ▼
<input type="button" value="Apply"/>	

Revision-level
<input type="text" value="0"/>

#### 4.23.2 Spanning-tree Port configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration**, and the following page appears. There are "PortFast configuration", "Port priority configuration", "Port cost configuration", "Spanning-tree port mode", "Link-type configuration", "Spanning-tree agreement port configuration", configuration web pages.



### 4.23.2.1 PortFast configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > PortFast configuration**, and the following page appears. You can set the any port to be PortFast.

PortFast configuration	
Port	Ethernet1/0/1 ▾
Operation	Add ▾
<div>Apply</div>	

PortFast configuration	
Port	PortType(1/0)
Ethernet1/0/1	1
Ethernet1/0/2	1
Ethernet1/0/3	1
Ethernet1/0/4	1
Ethernet1/0/5	1
Ethernet1/0/6	0
Ethernet1/0/7	0
Ethernet1/0/8	0
Ethernet1/0/9	0
Ethernet1/0/10	0
Ethernet1/0/11	0
Ethernet1/0/12	0
Ethernet1/0/13	0
Ethernet1/0/14	0
Ethernet1/0/15	0
Ethernet1/0/16	0
Ethernet1/0/17	0
Ethernet1/0/18	0

### 4.23.2.2 Port priority configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > Port priority configuration**, and the following page appears. You can set the priority and associate Instance to each port.

Port priority configuration	
Port	Ethernet1/0/1 ▾
Instance name	
Priority	
Operation	Default ▾
<div>Apply</div>	

Port priority configuration	
Ethernet1/0/1 of Instance 2	Operation port path cost 0, Port priority 48, Port Identifier 048.001
Ethernet1/0/2 of Instance 1	Operation port path cost 0, Port priority 16, Port Identifier 016.002

---

#### 4.23.2.3 Port cost configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > Port cost configuration**, and the following page appears. You can set the port cost and associate Instance to each port.

Port cost configuration	
Port	Ethernet1/0/1 ▾
Instance name	
Cost	
Operation	Default ▾
<div>Apply</div>	

Port cost configuration	
Ethernet1/0/1 of Instance 2	Operation port path cost 2222, Port priority 48, Port Identifier 048.001
Ethernet1/0/2 of Instance 1	Operation port path cost 33333, Port priority 16, Port Identifier 016.002

#### 4.23.2.4 Spanning-tree port mode.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > Spanning-tree port mode**, and the following page appears. You can force the port to work on SMTP mode.

Spanning-tree port mode	
Port	Ethernet1/0/1 ▾
<div>Apply</div>	

Information feedback window
switch# config t switch(config)# interface Ethernet1/0/1 switch(config-if-ethernet1/0/1)# spanning-tree mcheck

#### 4.23.2.5 Link-type configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > Link-type configuration**, and the following page appears. You can set the link type to auto, force-false or force-true for each port.



Link-type configuration	
Port	Ethernet1/0/1 ▾
Link type	auto ▾
Operation	Default ▾
<input type="button" value="Apply"/>	

Link-type configuration	
Port	Link type
Ethernet1/0/1	auto
Ethernet1/0/2	Force True
Ethernet1/0/3	Force False
Ethernet1/0/4	auto
Ethernet1/0/5	auto
Ethernet1/0/6	auto
Ethernet1/0/7	auto
Ethernet1/0/8	auto
Ethernet1/0/9	auto
Ethernet1/0/10	auto
Ethernet1/0/11	auto
Ethernet1/0/12	auto
Ethernet1/0/13	auto
Ethernet1/0/14	auto
Ethernet1/0/15	auto

#### 4.23.2.6 Spanning-tree agreement port configuration.

Choose **Spanning- tree configuration > Spanning-tree Port configuration > Spanning-tree agreement port configuration**, and the following page appears. You can enable or disable the spanning-tree function for each port.

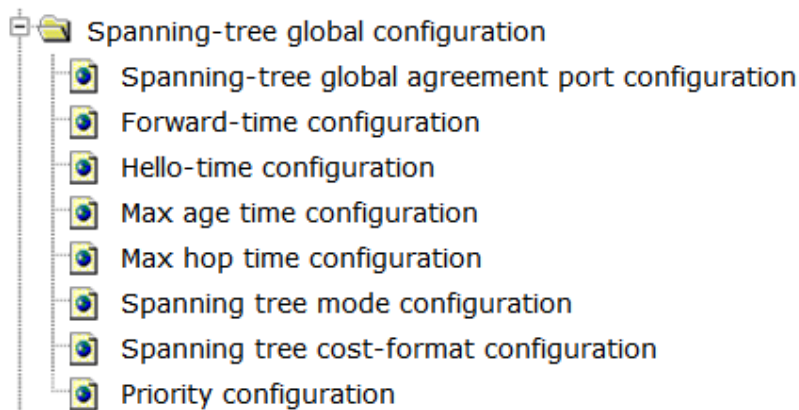
Spanning-tree agreement port configuration	
Port	Ethernet1/0/1 ▾
Operation	Disable ▾
<input type="button" value="Apply"/>	

Spanning-tree agreement port configuration	
Port	Spanning-tree agreement port configuration
Ethernet1/0/1	enable
Ethernet1/0/2	enable
Ethernet1/0/3	enable
Ethernet1/0/4	enable
Ethernet1/0/5	enable
Ethernet1/0/6	disable
Ethernet1/0/7	disable
Ethernet1/0/8	disable
Ethernet1/0/9	enable
Ethernet1/0/10	enable
Ethernet1/0/11	enable
Ethernet1/0/12	enable
Ethernet1/0/13	enable
Ethernet1/0/14	enable

---


### 4.23.3 Spanning-tree global configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration**, and the following page appears. There are "Spanning-tree global agreement port configuration", "Forward-time configuration", "Hello-time configuration", "Max age time configuration", "Max hop time configuration", "Spanning tree mode configuration", "Spanning tree cost-format configuration", "Priority configuration", configuration web pages.



#### 4.23.3.1 Spanning-tree global agreement port configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Spanning-tree global agreement port configuration**, and the following page appears. You can enable or disable Spanning-tree global agreement.



**TIPS**  
When spanning-tree global agreement configured, the port will be block, and then turn to forwarding; the web will be time-out, please relogin

#### 4.23.3.2 Forward-time configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Forward-time configuration**, You can set the forward-time, and notice that:  
 $2 \times (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$ ,  
 $\text{Bridge\_Max\_Age} \geq 2 \times (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$ .

Forward-time configuration	
Forward-time	<input type="text"/>
Operation	Default ▼
<input type="button" value="Apply"/>	

Forward-time configuration	
Forward-time configuration	15

#### 4.23.3.3 Hello-time configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Hello-time configuration**, and the following page appears. You can set Hello-time interval.

Hello-time configuration	
Bridge hello time	<input type="text"/>
Operation	Default ▼
<input type="button" value="Apply"/>	

Hello-time configuration	
Bridge hello time	2

#### 4.23.3.4 Max age time configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Max age time configuration**, and the following page appears. You can set Max age time.

Max age time configuration	
Max age time	<input type="text"/>
Operation	Default ▼
<input type="button" value="Apply"/>	

Max age time configuration	
Max age time	20

#### 4.23.3.5 Max hop time configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Max hop time configuration**, and the following page appears. You can set the Max hop

---

for BPDU.

Max hop time configuration	
Max hop time	
Operation	Default ▼
<div>Apply</div>	

Max hop time configuration	
Max hop time	20

#### 4.23.3.6 Spanning tree mode configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Spanning tree mode configuration**, and the following page appears. You can set the Spanning tree work mode to MSTP, STP or RSTP.

Spanning tree mode configuration	
Mode	Mstp ▼
Operation	Default ▼
<div>Apply</div>	

Spanning tree mode configuration	
Mode	mstp

#### 4.23.3.7 Spanning tree cost-format configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Spanning tree cost-format configuration**, and the following page appears. You can set the Spanning tree cost-format to dot1t or dot1d.

Spanning tree cost-format configuration	
Mode	dot1t ▼
<div>Apply</div>	

Spanning tree cost-format configuration	
Mode	dot1t

#### 4.23.3.8 Priority configuration.

Choose **Spanning- tree configuration > Spanning-tree global configuration > Priority configuration**, and the following page appears. You can set the priority for different

---

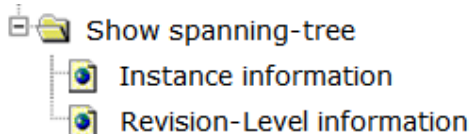
Instance.

Priority configuration	
Instance name	<input type="text"/>
Priority	<input type="text"/>
Operation	Default <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Priority configuration	
Instance name	Priority
0	32768

#### 4.23.4 Show Spanning-tree.

Choose **Spanning- tree configuration > Show Spanning-tree**, and the following page appears. There are "Instance information", "Revision-Level information", configuration web pages.



##### 4.23.4.1 Instance information.

Choose **Spanning- tree configuration > Show Spanning-tree > Instance information**, and the following page appears. You can show the detail information for Spanning-tree Instance.

Instance information	
Instance name	<input type="text"/>
<input type="button" value="Apply"/>	

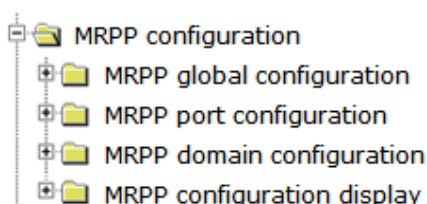
##### 4.23.4.2 Revision-Level information.

Choose **Spanning- tree configuration > Show Spanning-tree > Revision-Level information**, and the following page appears. You can show the Spanning-tree mst configuration information.

```
Information feedback window
switch# show spanning-tree mst config
Name
Revision      0
Instance      Vlans Mapped
-----
00            1-4094
-----
```

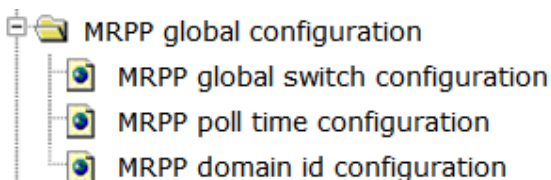
## 4.24 MRPP configuration.

Choose **MRPP configuration**, and the following page appears. There are "MRPP global configuration", "MRPP port configuration", "MRPP domain configuration", "MRPP configuration display", configuration web pages.



### 4.24.1 MRPP global configuration.

Choose **MRPP configuration > MRPP global configuration**, and the following page appears. There are "MRPP global switch configuration", "MRPP poll time configuration", "MRPP domain id configuration", configuration web pages.



#### 4.24.1.1 MRPP global switch configuration.

Choose **MRPP configuration > MRPP global configuration > MRPP global switch configuration**, and the following page appears. You can enable or disable the MRPP function.

MRPP global switch configuration	
Operation	Disable ▾
<div>Apply</div>	

MRPP global switch configuration	
MRPP global configuration	enable

---

#### 4.24.1.2 MRPP poll time configuration.

Choose **MRPP configuration > MRPP global configuration > MRPP poll time configuration**, and the following page appears. You can configure MRPP poll time.

MRPP poll time configuration	
MRPP poll time	<input type="text"/>
Operation	Default ▼
<input type="button" value="Apply"/>	

MRPP poll time configuration	
MRPP poll time	100

#### 4.24.1.3 MRPP domain id configuration.

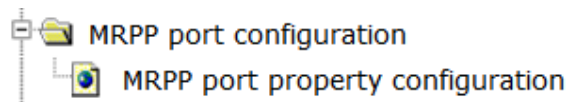
Choose **MRPP configuration > MRPP global configuration > MRPP domain id configuration**, and the following page appears. You can configure the domain ID for MRPP.

MRPP domain id configuration	
MRPP domain	<input type="text"/>
Operation	Remove ▼
<input type="button" value="Apply"/>	

MRPP domain id configuration	
Index	Domain ID

#### 4.24.2 MRPP port configuration.

Choose **MRPP configuration > MRPP port configuration**, and the following page appears.



#### 4.24.2.1 MRPP port property configuration.

Choose **MRPP configuration > MRPP port configuration > MRPP port property configuration**, and the following page appears. You can add or remove any port to MRPP

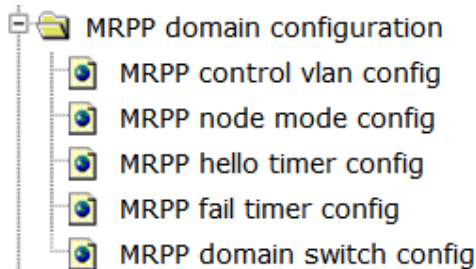
domain, and set the port property to primary or secondary.

MRPP port property configuration	
Port	Ethernet1/0/1 ▾
MRPP domain	
MRPP port property	primary ▾
Operation	Remove ▾
<div>Apply</div>	

MRPP port property configuration			
Index	Domain ID	Port Name	Property

### 4.24.3 MRPP domain configuration.

Choose **MRPP configuration > MRPP domain configuration**, and the following page appears. There are "MRPP control vlan config", "MRPP node mode config", "MRPP hello timer config", "MRPP fail timer config", "MRPP domain switch config", configuration web pages.



#### 4.24.3.1 MRPP control vlan config.

Choose **MRPP configuration > MRPP domain configuration > MRPP control vlan config**, and the following page appears. You can configure the MRPP control VLAN for MRPP domain.

MRPP control vlan config	
MRPP domain	▾
VLAN ID	
Operation	Remove ▾
<div>Apply</div>	

MRPP control vlan config		
Index	Domain ID	Control-VLAN



---

#### 4.24.3.2 MRPP node mode config.

Choose **MRPP configuration > MRPP domain configuration > MRPP node mode config**, and the following page appears. You can configure the MRPP ring node mode to master or transit.

MRPP node mode config	
MRPP domain	▼
MRPP node mode	master ▼
<div>Apply</div>	

MRPP node mode config		
Index	Domain ID	Node mode

#### 4.24.3.3 MRPP hello timer config.

Choose **MRPP configuration > MRPP domain configuration > MRPP hello timer config**, and the following page appears. You can set the MRPP hello timer range for the MRPP domain.

MRPP hello timer config	
MRPP domain	▼
MRPP hello timer range	
Operation	Remove ▼
<div>Apply</div>	

MRPP hello timer config		
Index	Domain ID	Hello-Timer

#### 4.24.3.4 MRPP fail timer config.

Choose **MRPP configuration > MRPP domain configuration > MRPP fail timer config > MRPP fail timer config**, and the following page appears. You can configure the MRPP hello message fail timer range for MRPP domain.

MRPP fail timer config	
MRPP domain	<input type="text"/>
MRPP fail timer range	<input type="text"/>
Operation	Remove <input type="text"/>
<input type="button" value="Apply"/>	

MRPP fail timer config		
Index	Domain ID	FAIL-Timer

#### 4.24.3.5 MRPP domain switch config.

Choose **MRPP configuration > MRPP domain configuration > MRPP domain switch config**, and the following page appears. You can enable or disable the MRPP domain.

MRPP node mode config	
MRPP domain	<input type="text"/>
Operation	Disable <input type="text"/>
<input type="button" value="Apply"/>	

MRPP domain switch configuration		
Index	Domain ID	Flag

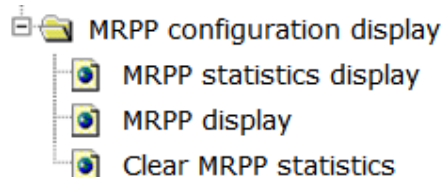
```

Information feedback window
switch# config t
switch(config)# mrpp ring 0
^
% Invalid input detected at '^' marker.
switch(config)# enable
% Incomplete command.

```

#### 4.24.4 MRPP configuration display.

Choose **MRPP configuration > MRPP configuration display**, and the following page appears. There are "MRPP statistics display", "MRPP display", "Clear MRPP statistics", configuration web pages.



---

#### 4.24.4.1 MRPP statistics display.

Choose **MRPP configuration > MRPP configuration display > MRPP statistics display**, and the following page appears. You can show the statistics information for each MRPP domain or for all domains.

MRPP statistics display	
MRPP domain	all ▼
<div>Apply</div>	

#### 4.24.4.2 MRPP display.

Choose **MRPP configuration > MRPP configuration display > MRPP display**, and the following page appears. You can show the configuration of the MRPP domain or all MRPP domains.

MRPP display	
MRPP domain	all ▼
<div>Apply</div>	

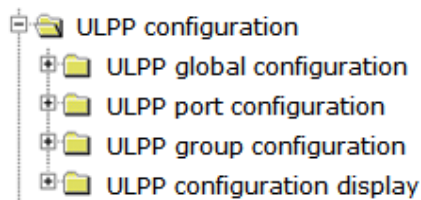
#### 4.24.4.3 Clear MRPP statistics.

Choose **MRPP configuration > MRPP configuration display > Clear MRPP statistics**, and the following page appears. You can clear the statistics for each MRPP domain or all domains.

Clear MRPP statistics	
MRPP domain	all ▼
<div>Apply</div>	

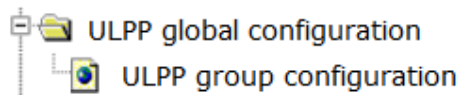
### 4.25 ULPP configuration.

Choose **ULPP configuration**, and the following page appears. There are "ULPP global configuration", "ULPP port configuration", "ULPP group configuration", "ULPP configuration display", configuration web pages.



#### 4.25.1 ULPP global configuration.

Choose **ULPP configuration > ULPP global configuration**, and the following page appears.



##### 4.25.1.1 ULPP group configuration.

Choose **ULPP configuration > ULPP global configuration > ULPP group configuration**, and the following page appears. You can add or remove ULPP group.

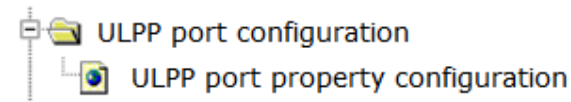
ULPP group configuration	
ULPP group	<input type="text"/>
Operation	Add ▼
<input type="button" value="Apply"/>	

ULPP group configuration
--------------------------

#### 4.25.2 ULPP port configuration.

Choose **ULPP configuration > ULPP port configuration**, and the following page appears.



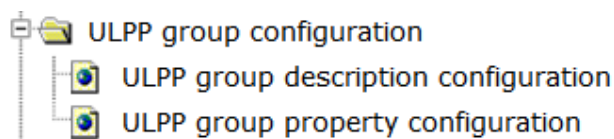
##### 4.25.2.1 ULPP port property configuration.

Choose **ULPP configuration > ULPP port configuration > ULPP port property configuration**, and the following page appears. You can configure the property for ULPP port, the flush mode could be mac or arp, and you can set the port as the master port or slave port.

ULPP port property configuration	
Port	Ethernet1/0/1 ▼
ULPP port flush mode	mac ▼ <input type="checkbox"/>
ULPP port control vlan	<input type="text"/> <input type="checkbox"/>
ULPP group	▼
ULPP port mode	master ▼ <input type="checkbox"/>
Operation	Remove ▼
<input type="button" value="Apply"/>	

### 4.25.3 ULPP group configuration.

Choose **ULPP configuration > ULPP group configuration**, and the following page appears. There are "ULPP description configuration", "ULPP group property configuration", configuration web pages.



#### 4.25.3.1 ULPP description configuration.

Choose **ULPP configuration > ULPP group configuration > ULPP description configuration**, and the following page appears. You can set description for ULPP group.

ULPP group description configuration	
ULPP group	▼
ULPP group description	<input type="text"/>
Operation	Remove ▼
<input type="button" value="Apply"/>	

ULPP group description configuration	
ULPP group	ULPP group description

#### 4.25.3.2 ULPP group property configuration.

Choose **ULPP configuration > ULPP group configuration > ULPP group property configuration**, and the following page appears. You can configure the property for ULPP group, the group preemption mode can be set to on or off, the flush mode could be mac or

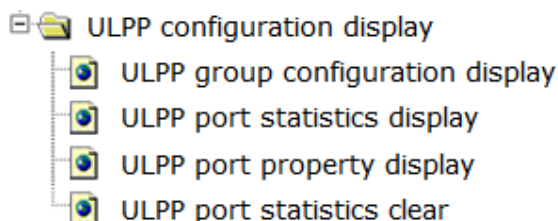
arp.

ULPP group property configuration	
ULPP group	<input type="text"/>
ULPP group preemption mode	on <input type="text"/>
ULPP group preemption delay	<input type="text"/>
ULPP group control vlan	<input type="text"/>
ULPP group protect vlan	<input type="text"/>
ULPP group flush mode	mac <input type="text"/>
Operation	Remove <input type="text"/>
<input type="button" value="Apply"/>	

ULPP group property configuration  
ULPP group|ULPP group preemption mode|ULPP group preemption delay|ULPP group control vlan|ULPP group flush mode

#### 4.25.4 ULPP configuration display.

Choose **ULPP configuration > ULPP configuration display**, and the following page appears. There are "ULPP group configuration display", "ULPP port statistics display", "ULPP port property display", "ULPP port statistics clear", configuration web pages.



##### 4.25.4.1 ULPP group configuration display.

Choose **ULPP configuration > ULPP configuration display > ULPP group configuration display**, and the following page appears. You can show the ULPP group configuration information.

ULPP group configuration display	
ULPP group	all <input type="text"/>
<input type="button" value="Apply"/>	

##### 4.25.4.2 ULPP port statistics display.

Choose **ULPP configuration > ULPP configuration display > ULPP port statistics display**, and the following page appears. You can show ULPP flush counter for each physical port or port-channel.

---

ULPP port statistics display	
Port	Ethernet1/0/1 ▾
<input type="button" value="Apply"/>	

#### 4.25.4.3 ULPP port property display.

Choose **ULPP configuration > ULPP configuration display > ULPP port property display**, and the following page appears. You can show ULPP flush-receive port list.

Information feedback window			
switch# show ulpp flush-receive-port			
ULPP flush-receive portlist:			
Portname	Type	Control	Vlan
-----			
-----			

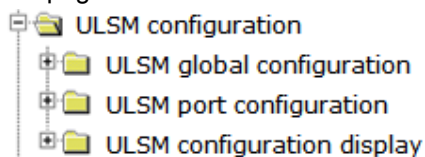
#### 4.25.4.4 ULPP port statistics clear.

Choose **ULPP configuration > ULPP configuration display > ULPP port statistics clear**, and the following page appears. You can clear ULPP flush counter for each physical port or port-channel.

ULPP port statistics clear	
Port	Ethernet1/0/1 ▾
<input type="button" value="Apply"/>	

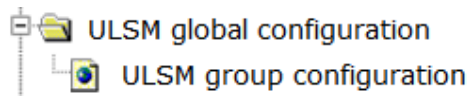
### 4.26 ULSM configuration.

Choose **ULSM configuration**, and the following page appears. There are "ULSM global configuration", "ULSM port configuration", "ULSM configuration display", configuration web pages.



#### 4.26.1 ULSM global configuration.

Choose **ULSM configuration > ULSM global configuration**, and the following page appears.



#### 4.26.1.1 ULSM group configuration.

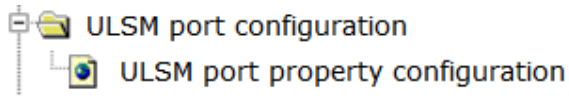
Choose **ULSM configuration > ULSM global configuration > ULSM group configuration**, and the following page appears. You can add or remove ULSM group.

ULSM group configuration	
ULSM group	<input type="text"/>
Operation	Add ▾
<input type="button" value="Apply"/>	

ULSM group configuration
--------------------------

#### 4.26.2 ULSM port configuration.

Choose **ULSM configuration > ULSM port configuration**, and the following page appears.



#### 4.26.2.1 ULSM port property configuration.

Choose **ULSM configuration > ULSM port configuration > ULSM port property configuration**, and the following page appears. You can add or remove a physical port or port-channel to ULSM group and set the property as downlink or uplink.

ULSM port property configuration	
Port	Ethernet1/0/1 ▾
ULSM group	▾
ULSM port property	downlink ▾
Operation	Remove ▾
<input type="button" value="Apply"/>	

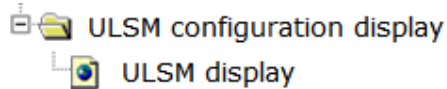
ULSM port property		
Port	ULSM group	ULSM port property



---

### 4.26.3 ULSM configuration display.

Choose **ULSM configuration > ULSM configuration display**, and the following page appears.



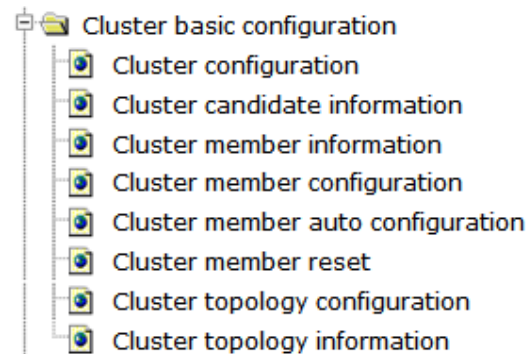
#### 4.26.3.1 ULSM display.

Choose **ULSM configuration > ULSM configuration display > ULSM display**, and the following page appears. You can show the state of ULSM group.



### 4.27 Cluster basic configuration.

Choose **Cluster basic configuration**, and the following page appears. There are "Cluster configuration", "Cluster candidate information", "Cluster member information", "Cluster member configuration", "Cluster member auto configuration", "Cluster member reset", "Cluster topology configuration", "Cluster topology information", configuration web pages.



#### 4.27.1 Cluster configuration.

Choose **Cluster basic configuration > Cluster configuration**, and the following page appears. You can enable cluster and configure key, VLAN ID, name, IP pool, auto add member, keepalive interval and loss count for the Cluster.

Cluster state configuration	
Cluster Status	<input type="checkbox"/> Enabled
Cluster Key	<input type="text"/>
Cluster Vlan ID (1-4094)	<input type="text"/>
<input type="button" value="Apply"/>	

Cluster commander configuration	
Cluster Commander	<input type="checkbox"/> Enabled
Cluster Name	<input type="text"/>
<input type="button" value="Apply"/>	

Cluster ip-pool configuration	
Cluster IP Pool	<input type="text"/>
<input type="button" value="Apply"/>	

Cluster auto-add configuration	
Auto Add Members	<input type="checkbox"/> Enabled
<input type="button" value="Apply"/>	

Cluster keepalive interval configuration	
Keepalive Interval (3-30)	<input type="text"/> Seconds
<input type="button" value="Apply"/>	

Cluster keepalive losscount configuration	
Keepalive Loss Count (1-10)	<input type="text"/>
<input type="button" value="Apply"/>	

Cluster configuration	
Role	<input type="text"/>
Cluster Key	<input type="text"/>
Number of Members	0
Number of Candidates	0

#### 4.27.2 Cluster candidate information.

Choose **Cluster basic configuration > Cluster candidate information**, and the following page appears. You can see the Cluster candidate information.

Cluster candidate information		
Hostname	MAC Address	Description

#### 4.27.3 Cluster member information.

Choose **Cluster basic configuration > Cluster member information**, and the following page appears. You can see the Cluster member information.

Cluster member information						
Member ID	Hostname	MAC Address	Internal IP Address	Type	Status	Description
5		00-00-00-00-00-01	0.0.0.0	User	Inactive	
6		00-00-00-00-00-02	0.0.0.0	User	Inactive	

#### 4.27.4 Cluster member configuration.

Choose **Cluster basic configuration > Cluster member configuration**, and the following page appears. You can add or remove member to the Cluster group.

Cluster member configuration	
Current Cluster Member List:	Add new Cluster Member:
<input type="checkbox"/> ID 5, 00-00-00-00-00-01 <input type="checkbox"/> ID 6, 00-00-00-00-00-02	<input type="button" value="Add"/> <input type="button" value="Remove"/>
	Member ID (1-128) <input type="text"/> MAC Address (XX-XX-XX-XX-XX-XX) <input type="text"/> <input checked="" type="radio"/> Candidate Table

---

#### 4.27.5 Cluster member auto configuration.

Choose **Cluster basic configuration > Cluster member auto configuration**, and the following page appears. You can Convert auto-add cluster members into user-config members vice versa.

Cluster member auto configuration	
Convert auto-add cluster members into user-config members.	
	<input type="button" value="Convert"/>

Information feedback window
switch# config t switch(config)# cluster member auto-to-user

#### 4.27.6 Cluster member reset.

Choose **Cluster basic configuration > Cluster member reset**, and the following page appears. You can reset the member switch by using this command on command switch.

Cluster member reset
<input type="button" value="Apply"/>

#### 4.27.7 Cluster topology configuration.

Choose **Cluster basic configuration > Cluster topology configuration**, and the following page appears. You can configure the Cluster topology.



#### 4.27.8 Cluster topology information.

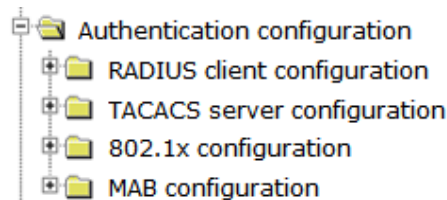
Choose **Cluster basic configuration > Cluster topology information**, and the following page appears. You can show the cluster topology information and clear the cluster table.

Cluster topology information							
Serial Number	Role	Hostname	MAC Address	Upstream Local Port	Upstream Remote Port	Leaf Node	Description
-	Commander	switch	00-e0-53-16-d0-01	-root-	-root-	-	FR-S3028PETF-C
1	Unknow		00-00-00-00-00-01			Yes	
2	Unknow		00-00-00-00-00-02			Yes	

Clear cluster table.

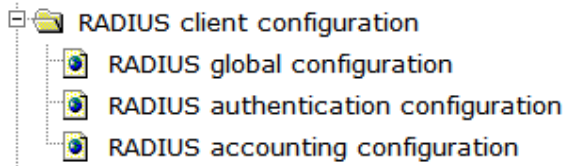
## 4.28 Authentication configuration.

Choose **Authentication configuration**, and the following page appears. There are "RADIUS client configuration", "TACACS server configuration", "802.1x configuration", "MAB configuration", configuration web pages.



### 4.28.1 RADIUS client configuration.

Choose **Authentication configuration > RADIUS client configuration**, and the following page appears. There are "RADIUS global configuration", "RADIUS authentication configuration", "RADIUS accounting configuration", configuration web pages.



#### 4.28.1.1 RADIUS global configuration.

Choose **Authentication configuration > RADIUS client configuration > RADIUS global configuration**, and the following page appears. You can set the radius global configuration.

RADIUS configuration	
Authentication status	Enable ▼
Accounting	Disable ▼
Radius key operation	▼
RADIUS key	22
System recovery time	5
RADIUS Retransmit times	3
RADIUS server timeout	3
Apply	

AAA server status	
the status of the aaa	enable
the status of the radius accounting	disable
radius-server timeout	3
radius-server retransmit	3
radius-server dead-time	5
radius-server key	22
radius-server authentication host	192.168.5.10 port:8282 primary

```

switch# config t
switch(config)# aaa-accounting enable
ERROR: invalid, you should config at least one radius accounting server
switch# config t
switch(config)# radius-server key 22
switch# config t
switch(config)# radius-server dead-time 5
switch# config t
switch(config)# radius-server retransmit 3
switch# config t
switch(config)# radius-server timeout 3

```

#### 4.28.1.2 RADIUS authentication configuration.

Choose **Authentication configuration > RADIUS client configuration > RADIUS authentication configuration**, and the following page appears. You can set the information of the primary and non-primary Radius authentication server.

RADIUS authentication server configuration	
Authentication server IP	
Authentication server port(optional)	
Primary authentication server	Primary authentication server ▼
Operation	Add ▼
Apply	

RADIUS server configuration list		
Server IP	Port num	Primary server

#### 4.28.1.3 RADIUS accounting configuration.

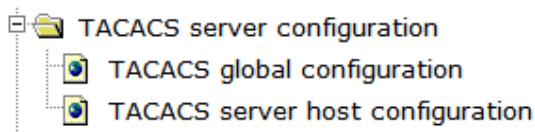
Choose **Authentication configuration > RADIUS client configuration > RADIUS accounting configuration**, and the following page appears. You can set the information of the primary and non-primary Radius accounting server.

RADIUS accounting server configuration	
Accounting server IP	<input type="text"/>
Accounting server port(optional)	<input type="text"/>
Primary accounting server	Primary accounting server ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

RADIUS accounting server configuration list		
Server IP	Port num	Primary server

## 4.28.2 TACACS server configuration.

Choose **Authentication configuration > TACACS server configuration**, and the following page appears. There are "TACACS global configuration", "TACACS server host configuration", configuration web pages.



### 4.28.2.1 TACACS global configuration.

Choose **Authentication configuration > TACACS server configuration > TACACS global configuration**, and the following page appears. You can set the TACACS server configuration.

TACACS configuration	
TACACS key	<input type="text"/>
TACACS server timeout	3 <input type="text"/>
Operation	Remove ▼
<input type="button" value="Apply"/>	

TACACS server status	
the status of the tacacs	
tacacs-server timeout	3

### 4.28.2.2 TACACS server host configuration.

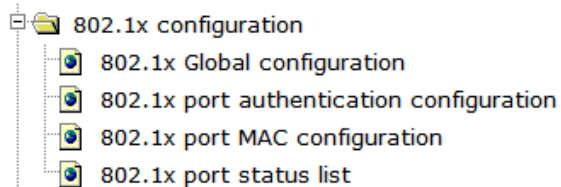
Choose **Authentication configuration > TACACS server configuration > TACACS server host configuration**, and the following page appears. You can set the information of the primary and non-primary TACACS authentication server.

TACACS server configuration	
Authentication server IP	<input type="text"/>
Authentication server port(optional)	<input type="text"/>
Primary authentication server	Primary authentication server ▼
Operation	Add ▼
<input type="button" value="Apply"/>	

TACACS server configuration list		
Server IP	Port num	Primary server

### 4.28.3 802.1x configuration.

Choose **Authentication configuration > 802.1x configuration**, and the following page appears. There are "802.1x Global configuration", "802.1x port authentication configuration", "802.1x port MAC configuration", "802.1x port status list", configuration web pages.



#### 4.28.3.1 802.1x Global configuration.

Choose **Authentication configuration > 802.1x configuration > 802.1x Global configuration**, and the following page appears. You can set the 802.1X global configuration, the EAP relay authentication mode, Private client and MAC filtering can be set to permit or forbid.

802.1x configuration	
802.1x status	Enable ▾
Maximum retransmission times of EAP-request/identity	2
Reauthenticate client periodically	Enable ▾
Holddown time for authentication failure	10
Reauthenticate client interval	3600
Resending EAP-request/identity interval	30
EAP relay authentication mode	forbid ▾
Private client	forbid ▾
MAC filtering	forbid ▾
802.1x unicast	Enable ▾
Apply	

```

Information feedback window
switch# show dot1x
Global 802.1X Parameters
  free resource      :unknown
  reauth-enabled     :yes
  reauth-period      :3600
  quiet-period       :10
  tx-period          :30
  max-req            :2
  authenticator mode :active
Mac Filter Disable
MacAccessList :
dot1x-EAPoR Disable
dot1x-privateclient Disable
dot1x-privateclient protect Disable
dot1x-unicast Enable
dot1x-web authentication Disable
  
```

#### 4.28.3.2 802.1x port authentication configuration.

Choose **Authentication configuration > 802.1x configuration > 802.1x port authentication configuration**, and the following page appears. You can configure the 802.1x authentication for each port, the Authentication mode can be force-unauthorized, Auto(802.1X) or force-authorized, the Authentication mode can be Port-based or MAC-based.

802.1x port configuration	
Port	Ethernet1/0/1 ▾
802.1x status	Disable ▾
Authentication type	force-unauthorized ▾
Authentication mode	Port-based ▾
Port maximum user	1
Guest VLAN ID	0
Apply	

```

Information feedback window
switch# show dot1x interface Ethernet1/0/1
802.1X is disabled on port Ethernet1/0/1
  
```



---

#### 4.28.3.3 802.1x port MAC configuration list.

Choose **Authentication configuration > 802.1x configuration > 802.1x port MAC configuration**, and the following page appears. You can set a MAC address to add MAC filter entry or remove MAC filter entry for each port.

802.1x port MAC configuration	
Port	Ethernet1/0/1 ▾
Mac	<input type="text"/>
Operation	Add MAC filter entry ▾
<input type="button" value="Apply"/>	

802.1x port MAC filter entry	
Port	mac

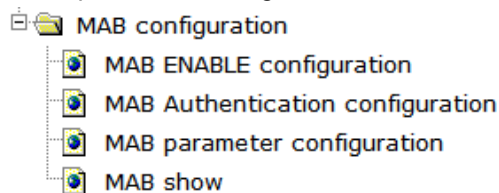
#### 4.28.3.4 802.1x port status list.

Choose **Authentication configuration > 802.1x configuration > 802.1x port status list**, and the following page appears. You can show the 802.1X authentication status of each port or reauthenticate the port.

802.1x port status list	
Port	Ethernet1/0/1 ▾
802.1x status	Disable
Authentication type	NULL
Authentication status	Unauthenticated
Authentication mode	No authentication mode
<input type="button" value="Reauthenticate"/>	

#### 4.28.4 MAB configuration.

Choose **Authentication configuration > MAB configuration**, and the following page appears. There are "MAB ENABLE configuration", "MAB Authentication configuration", "MAB parameter configuration", "MAB show", configuration web pages.



##### 4.28.4.1 MAB ENABLE configuration.

Choose **Authentication configuration > MAB configuration > MAB ENABLE configuration**, and the following page appears. You can enable or disable the mac-authentication-bypass function for global or each port.

MAB global enable configuration	
MAB global enable	Enable
<input type="button" value="Apply"/>	

MAB port enable configuration	
Port	Ethernet1/0/1
MAB port enable	Enable
<input type="button" value="Apply"/>	

#### 4.28.4.2 MAB Authentication configuration.

Choose **Authentication configuration > MAB configuration > MAB Authentication configuration**, and the following page appears. You can set the MAB authentication type to MAC address or username and password.

MAB Authentication configuration	
MAB Authentication TYPE	MAC address
username	
password	
<input type="button" value="Apply"/>	

#### 4.28.4.3 MAB parameter configuration.

Choose **Authentication configuration > MAB configuration > MAB parameter configuration**, and the following page appears. You can set MAB parameter.

MAB parameter configuration	
Port	Ethernet1/0/1
parameter type	guest vlan range
value	
Enable	
<input type="button" value="Apply"/>	

MAB parameter configuration	
parameter type	reauth-period
value	
Enable	
<input type="button" value="Apply"/>	

authentication mab	
check type	radius
Enable	
<input type="button" value="Apply"/>	

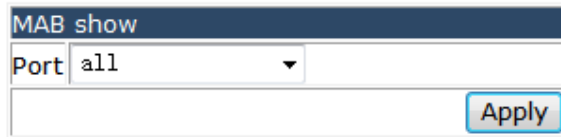
spoofing-garp-check	
spoofing-garp-check	Enable
<input type="button" value="Apply"/>	

MAB show	
guest vlan range	1-4094
max binding value	1-100
reauth-period	1-3600
offline-detect	0 60-7200
quiet-period	1-60
stale-period	0-60
linkup-period	0-30

---

#### 4.28.4.4 MAB show.

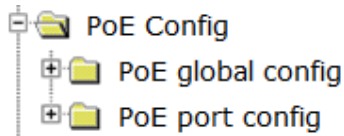
Choose **Authentication configuration > MAB configuration > MAB show**, and the following page appears. You can show the MAB information for each port or all ports.

The image shows a web interface titled "MAB show". It contains a label "Port" followed by a dropdown menu currently set to "all". Below the dropdown is a large empty rectangular area. To the right of this area is a blue button with the text "Apply".

MAB show	
Port	all
<div> </div>	
<div>Apply</div>	

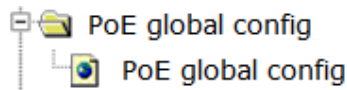
#### 4.29 PoE Config.

Choose **PoE Config**, and the following page appears. There are "PoE global config", "PoE port config", configuration web pages.



##### 4.29.1 PoE global config.

Choose **PoE Config > PoE global config**, and the following page appears. There are "PoE global config", configuration web pages.



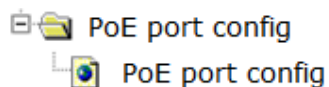
##### 4.29.1.1 PoE global config

1. Choose **PoE Config > PoE global config > PoE global config**, and the following page appears. You can set the POE global configuration..

PoE global config	
Power Inline Status	off ▼
Power Available(37-370 W)	0
Power Used	0 W
Power Remaining	0 W
Min Voltage	0 V
Max Voltage	0 V
Police	off ▼
Legacy	off ▼
high-inrush Status	enable ▼
Disconnect	ac
Mode	spare
HW Version	1
SW Version	1
monitor interval(30-36000 s)	150
reset interval(1-600 s)	5
<input type="button" value="Apply"/>	

#### 4.29.2 PoE port config.

Choose **PoE Config > PoE port config**, and the following page appears. There are "**PoE port config**", configuration web pages.



##### 4.29.2.1 PoE port config

2. Choose **PoE Config > PoE port config > PoE port config**, and the following page appears. You can set the POE parameters for each port, the status could be auto, static and disable, the priority could be low, high or critical.

PoE port config			
Interface	Status	Priority	monitor status
Ethernet1/0/1	auto	low	off

[Apply](#)

Max Power	
Interface	Max Power(1-30000mW)
Ethernet1/0/1	30000 mW

[Apply](#)

Time range name	
Interface	Time range name
Ethernet1/0/1	

[Apply](#)

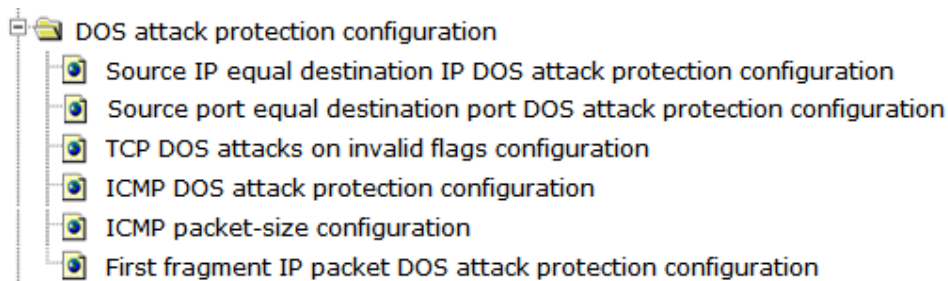
Unset Time range name	
Interface	
Ethernet1/0/1	

[Default](#)

Interface	Status	Oper	Power(mW)	Max Power(1-30000mW)	Current(mA)	Volt(V)	Priority	Class	Time range name
Ethernet1/0/1	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/2	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/3	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/4	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/5	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/6	disable	faulty	-1	0	-1	-1	critical	-1	NULL
Ethernet1/0/7	disable	faulty	-1	0	-1	-1	critical	-1	NULL

## 4.30 DOS attack protection configuration.

Choose **DOS attack protection configuration**, and the following page appears. There are "Source IP equal destination IP DOS attack protection configuration", "Source port equal destination port DOS attack protection configuration", "TCP DOS attacks in invalid flags configuration", "ICMP DOS attack protection configuration", "ICMP packet-size configuration", "First fragment IP packet DOS attack protection configuration", configuration web pages.



### 4.30.1 Source IP equal destination IP DOS attack protection configuration.

Choose **DOS attack protection configuration > Source IP equal destination IP DOS attack protection configuration**, and the following page appears. You can enable or disable the protection function for DOS attack with source IP equal destination IP.

---

Source IP equal destination IP DOS attack protection configuration	
DOS attack protection status	Enable ▾
<div>Apply</div>	

DOS attack protection status	
DOS attack protection status	Enable

Information feedback window
switch# config t switch(config)# dosattack-check srcip-equal-dstip enable

#### 4.30.2 Source port equal destination port DOS attack protection configuration.

Choose **DOS attack protection configuration > Source port equal destination port DOS attack protection configuration**, and the following page appears. You can enable or disable the protection function for DOS attack with source port equal destination port.

Source port equal destination port DOS attack protection configuration	
DOS attack protection status	Enable ▾
<div>Apply</div>	

DOS attack protection status	
DOS attack protection status	Enable

#### 4.30.3 TCP DOS attacks on invalid flags configuration.

Choose **DOS attack protection configuration > TCP DOS attacks on invalid flags configuration**, and the following page appears. You can enable or disable the protection function for TCP DOS attacks on invalid flags.

---

TCP DOS attacks on invalid flags configuration	
DOS attack protection status	Enable ▾
<div>Apply</div>	

DOS attack protection status	
DOS attack protection status	Enable

#### 4.30.4 ICMP DOS attack protection configuration.

Choose **DOS attack protection configuration > ICMP DOS attack protection configuration**, and the following page appears. You can enable or disable the protection function for ICMP DOS attack.

ICMP DOS attack protection configuration	
DOS attack protection status	Enable ▾
<div>Apply</div>	

DOS attack protection status	
DOS attack protection status	Enable

#### 4.30.5 ICMP packet-size configuration.

Choose **DOS attack protection configuration > ICMP packet-size configuration**, and the following page appears. You can set the ICMP packet-size for ICMP DOS attack protection.

ICMP packet-size configuration	
Packet-size	<input type="text"/>
<input type="button" value="Apply"/>	

Packet-size	
Packet-size	512

#### 4.30.6 First fragment IP packet DOS attack protection configuration.

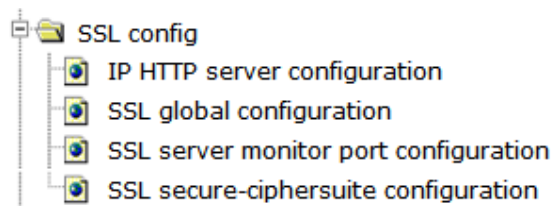
Choose **DOS attack protection configuration > First fragment IP packet DOS attack protection configuration**, and the following page appears. You can enable or disable the protection function for first fragment IP packet DOS attack.

First fragment IP packet DOS attack protection configuration	
DOS attack protection status	Enable ▼
<input type="button" value="Apply"/>	

DOS attack protection status	
DOS attack protection status	Enable

#### 4.31 SSL config.

Choose **SSL config**, and the following page appears. There are "IP HTTP server configuration", "SSL global configuration", "SSL server monitor port configuration", "SSL secure-ciphersuite configuration", configuration web pages.





---

#### 4.31.1 IP HTTP server configuration.

Choose **SSL config > IP HTTP server configuration**, and the following page appears. You can enable or disable the IP HTTP server.

IP HTTP server configuration	
IP HTTP server status	Enable ▼
<div>Apply</div>	

Information feedback window	
IP HTTP server status	Enable

#### 4.31.2 SSL global configuration.

Choose **SSL config > SSL global configuration**, and the following page appears. You can enable or disable the SSL function.

SSL global configuration	
SSL status	Enable ▼
<div>Apply</div>	

Information feedback window	
SSL status	Enable

#### 4.31.3 SSL server monitor port configuration.

Choose **SSL config > SSL server monitor port configuration**, and the following page appears. You can set the SSL server monitor port.

SSL server monitor port configuration	
port number	<input type="text"/>
Operation	Add ▼
<div>Apply</div>	

Information feedback window	
port number	443

#### 4.31.4 SSL secure-ciphersuite configuration.

Choose **SSL config > SSL secure-ciphersuite configuration**, and the following page

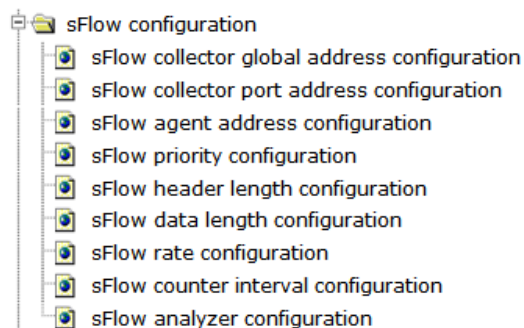
appears. You can configure the SSL secure-ciphersuite type to des-cbc3-sha, rc4-128-sha or des-cbc-sha.

secure-ciphersuite configuration	
secure-ciphersuite type	des-cbc3-sha ▼
Operation	Add ▼
<div>Apply</div>	

Information feedback window
ip http secure-ciphersuite RC4-MD5

## 4.32 sFLOW configuration.

Choose **sFLOW configuration**, and the following page appears. There are "sFLOW collector global address configuration", "sFLOW collector port address configuration", "sFLOW agent address configuration", "sFLOW priority configuration", "sFLOW header length configuration", "sFLOW data length configuration", "sFLOW rate configuration", "sFLOW counter interval configuration", "sFLOW analyzer configuration", configuration web pages.



### 4.32.1 sFLOW collector global address configuration.

Choose **sFLOW configuration > sFLOW collector global address configuration**, and the following page appears. You can set the sFLOW collector global address and destination port.

sFlow collector global address configuration	
IP address	<input type="text"/>
destination port NO.	<input type="text"/>
Operation	Configuration ▼
<div>Apply</div>	

---

#### 4.32.2 sFLOW collector port address configuration.

Choose **sFLOW configuration > sFLOW collector port address configuration**, and the following page appears. You can set the IP address and destination port for each physical port.

sFlow collector port address configuration	
Port	Ethernet1/0/1 ▾
IP address	<input type="text"/>
destination port NO.	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.32.3 sFLOW agent address configuration.

Choose **sFLOW configuration > sFLOW agent address configuration**, and the following page appears. You can set the address of the sFLOW agent.

sFlow agent address configuration	
IP address	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.32.4 sFLOW priority configuration.

Choose **sFLOW configuration > sFLOW priority configuration**, and the following page appears. You can set the priority of the sFLOW agent.

sFlow priority configuration	
agent priority value	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.32.5 sFLOW header length configuration.

Choose **sFLOW configuration > sFLOW header length configuration**, and the following page appears. You can set the sFLOW header length.

---

sFlow header length configuration	
Port	Ethernet1/0/1 ▾
header length	<input type="text"/>
Operation	Configuration ▾
<div>Apply</div>	

#### 4.32.6 sFLOW data length configuration.

Choose **sFLOW configuration > sFLOW data length configuration**, and the following page appears. You can set the sFLOW data length.

sFlow data length configuration	
Port	Ethernet1/0/1 ▾
data length	<input type="text"/>
Operation	Configuration ▾
<div>Apply</div>	

#### 4.32.7 sFLOW rate configuration.

Choose **sFLOW configuration > sFLOW rate configuration**, and the following page appears. You can set sFLOW rate value for direction input and output.

sFlow rate configuration	
Port	Ethernet1/0/1 ▾
direction	input ▾
rate value	<input type="text"/>
Operation	Configuration ▾
<div>Apply</div>	

#### 4.32.8 sFLOW counter interval configuration.

Choose **sFLOW configuration > sFLOW counter interval configuration**, and the following page appears. You can set sFLOW counter interval.

sFlow counter interval configuration	
Port	Ethernet1/0/1 ▾
counter interval	<input type="text"/>
Operation	Configuration ▾
<input type="button" value="Apply"/>	

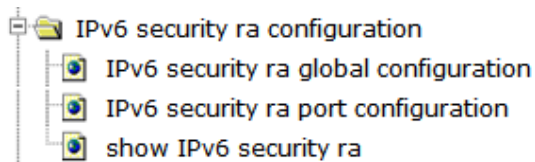
#### 4.32.9 sFLOW analyzer configuration.

Choose **sFLOW configuration > sFLOW analyzer configuration**, and the following page appears. You can configure or remove the sflowtrend sFLOW analyzer.

sFlow analyzer configuration	
Operation	Configuration ▾
<input type="button" value="Apply"/>	

#### 4.33 IPv6 security ra configuration.

Choose **IPv6 security ra configuration**, and the following page appears. There are "IPv6 security ra global configuration", "IPv6 security ra port configuration", "Show IPv6 security ra", configuration web pages.



##### 4.33.1 IPv6 security ra global configuration.

Choose **IPv6 security ra configuration > IPv6 security ra global configuration**, and the following page appears. You can enable or disable the IPv6 security ra function..

IPv6 security ra global configuration	
Operation	Enable ▾
<input type="button" value="Apply"/>	

##### 4.33.2 IPv6 security ra port configuration.

Choose **IPv6 security ra configuration > IPv6 security ra port configuration**, and the

---

following page appears. You can enable or disable the IPv6 security ra for each physical port.

IPv6 security ra port configuration	
Port	Ethernet1/0/1 ▼
Operation	Enable ▼
<div>Apply</div>	

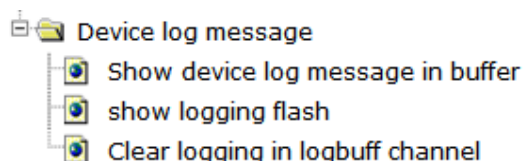
### 4.33.3 Show IPv6 security ra.

Choose **IPv6 security ra configuration > Show IPv6 security ra**, and the following page appears. You can show the IPv6 security state for each port or all ports.

show IPv6 security ra	
Port	Ethernet1/0/1 ▼
<div>Apply</div>	

## 4.34 Device log message.

Choose **Device log message**, and the following page appears. There are "Show device log message in buffer", "Show logging flash", "Clear logging in logbuff channel", configuration web pages.



### 4.34.1 Show device log message in buffer.

Choose **Device log message > Show device log message in buffer**, and the following page appears. You can show the device log message with level critical or warning, and you can choose the ID range of the message.

Show device log message in buffer	
Level	critical ▼
Begin	<input type="text"/>
End	<input type="text"/>
<div>Apply</div>	

---

### 4.34.2 Show logging flash.

Choose **Device log message > Show logging flash**, and the following page appears. You can show the logging flash.

```
Information feedback window
switch# show logging flash
Allowed max messages:512,Current messages:512
512 %Jan 01 03:54:21 2006 <warnings> MODULE_CONFIG_WEB[tWebCfg]:HTTP: User admin, login successfully from 192.168.2.22.
511 %Jan 01 03:45:52 2006 <warnings> MODULE_CONFIG_WEB[tWebCfg]:HTTP: User admin, login successfully from 192.168.2.22.
510 %Jan 01 03:45:47 2006 <warnings> MODULE_CONFIG_WEB[tWebCfg]:HTTP: User admin, login successfully from 192.168.2.22.
509 %Jan 01 01:56:52 2006 <warnings> DEFAULT[tIPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
508 %Jan 01 01:56:51 2006 <warnings> MODULE_L2_MSTP[tMstp]:MSTP set port = 7, mst = 0 to FORWARDING!
507 %Jan 01 01:56:36 2006 <warnings> MODULE_L2_MSTP[tMstp]:MSTP set port = 7, mst = 0 to LEARNING!
506 %Jan 01 01:56:21 2006 <warnings> DEFAULT[tIPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to DOWN
505 %Jan 01 00:09:09 2006 <warnings> MODULE_CONFIG_WEB[tWebCfg]:HTTP: User admin, login successfully from 192.168.2.22.
504 %Jan 01 00:00:21 2006 <critical> DEFAULT[zIMI]:System cold restart...
503 %Jan 01 00:00:14 2006 <warnings> DEFAULT[tIPTimer]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,changed state to UP
502 %Jan 01 00:00:13 2006 <warnings> MODULE_PORT[tphyDaemon]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/7, changed state to UP
501 %Jan 01 00:00:11 2006 <warnings> MODULE_PORT[zIMI]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/28, changed state to DOWN
500 %Jan 01 00:00:11 2006 <warnings> MODULE_PORT[zIMI]:%LINK-5-CHANGED: Interface Ethernet1/0/28, changed state to UP
499 %Jan 01 00:00:11 2006 <warnings> MODULE_PORT[zIMI]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/27, changed state to DOWN
498 %Jan 01 00:00:11 2006 <warnings> MODULE_PORT[zIMI]:%LINK-5-CHANGED: Interface Ethernet1/0/27, changed state to UP
497 %Jan 01 00:00:11 2006 <warnings> MODULE_PORT[zIMI]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0/26, changed state to DOWN
496 %Jan 01 00:00:11 2006 <warnings> MODULE_PORT[zIMI]:%LINK-5-CHANGED: Interface Ethernet1/0/26, changed state to UP
```

### 4.34.3 Clear logging in logbuff channel.

Choose **Device log message > Clear logging in logbuff channel**, and the following page appears. You can clear the logging in the logbuff channel..

Clear logging in logbuff channel

Clear logging in logbuff channel?

---

## **Appendix: Technical Specifications**

Specification		
Standards		IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3az, IEEE802.3ae.
Number of Ports		24 x 10/100/1000Mbps Auto-Negotiation ports 4 x 1000/10000Mbps SFP+ ports
Network Media (Cable)		10Base-T: UTP category 3, 4, 5 cable (maximum 100m) 100Base-Tx: UTP category 5, 5e cable (maximum 100m) 1000Base-T: UTP category 5e, 6 cable (maximum 100m) 10GBase-LR 10GBase-SR
capability	Store-and-Forward	Supports
	Switching Capacity	128Gbps
	MAC Address Learning	Automatically learning, automatically Update 16K Table
Environment		Operating Temperature: 0℃~40℃ Storage Temperature: -40℃~70℃ Operating Humidity: 10%~90% non-condensing Storage humidity: 5%~95% non-condensing
LED indicators	Per-Port	Link/Act : 10/100/10000Mbps:Green
	Other	Power: Green
Dimensions (W × D × H)		440x330x44mm (19 metal case)
Power		AC 100V~240V 50/60HZ 1A (Internal Power supply)





[www.morrelltelecom.com](http://www.morrelltelecom.com)

[sales@morrelltelecom.com](mailto:sales@morrelltelecom.com)

[morrelltelecom](#)

