MR-800K SERIES

8-Gigabit PoE Port + 2-Gigabit SFP Port

사용자 매뉴얼

Ver. 1.0

Revision history

일자	버전	설명
2024-08-29	V 1.0	최초 작성

※ 본 문서는 Firmware 버전 1.0.1.11 을 기준으로 작성되었으며, 펌웨어에 따라 WEB UI 의 디자인 및 메뉴 구성에 차이가 있을 수 있습니다.

Contents

MR-800K SERIES 1
8-Gigabit PoE Port + 2-Gigabit SFP Port 1
사용자 매뉴얼 1
Ver. 1.0 1
1 소개 및 설치 10
1.1 제품 주요 사양 10
1.2 제품 구성품 12
1.3 제품 외관 12
1.4 제품 설치 13
1.5 안전을 위한 주의 사항 13
2 Web Page Login 15
2.1 네트워크 관리 클라이언트에 로그인 15
2.2 클라이언트 인터페이스 구성 15
2.3 웹 인터페이스의 탐색 트리 16
3 Status 22
3.1 System Information 22
3.2 Statistics 23
3.3 MAC Address Table 24
3.4 Reboot 25
4 Network 26
4.1 IP Address 26
4.2 DNS 26
4.3 System Time 28
5 Port 29
5.1 Port Setting 29
5.2 Error Disabled 30
5.3 Link Aggregation 31
5.3.1 Group 33

5.3.2 Port Setting 35
5.3.3 LACP 35
5.4 EEE 38
5.5 Jumbo Frame 39
5.6 Port Security 39
5.7 Protected Port 40
5.8 Storm Control 41
5.9 Mirroring 43
6 POE Setting 44
6.1 PoE Port Setting 45
6.2 POE Port Timer Setting 46
6.3 POE Port Timer Reboot Setting 46
7 VLAN 47
7.1 VLAN 48
7.1.1 Create VALN 48
7.1.2 VLAN Configuration 49
7.1.3 Membership 50
7.1.4 Port Setting 52
7.2 Voice VLAN 54
7.3 Protocol VLAN 59
7.4 MAC VLAN 64
7.5 Surveillance VLAN 67
7.6 GVRP 69
7.6.1 Property 70
7.6.2 Membership 71
7.6.3 Statistics 72
8 MAC Address Table 73
8.1 Dynamic Address 73
8.2 Static Address 75
8.3 Filtering Address 75

8.4 Port Security Address 76
9 Spanning Tree 77
9.1 Property 78
9.2 Port Setting 79
9.3 MST Instance 81
9.4 MST Port Setting 83
9.5 Statistics 87
10 Discovery 87
10.1 LLDP 88
10.2 Port Setting 89
10.3 MED Network Policy 91
10.4 MED Port Setting 92
10.5 Packet View 93
10.6 Local Information 94
10.7 Neighbor 95
10.8 Statistics 95
11 DHCP 96
11.1 Property 99
11.2 IP Pool Setting 99
11.3 VLAN IF Address Group Setting 100
11.4 Client List 101
11.5 Client Static Binding Table 102
12 Multicast 102
12.1 General 102
12.1.1 Property 102
12.1.2 Group Address 103
12.1.3 Router Port 104
12.1.4 Forward All 105
12.1.5 Throttling 105
12.1.6 Filtering Profile 106

12.2 IGMP Snooping 106
12.2.1 Property 107
12.2.2 Querier 109
12.2.3 Statistics 109
12.3 MLD Snooping 110
12.3.1 Property 111
12.3.2 Statistics 113
12.4 MVR 113
12.4.1 Property 114
12.4.2 Port Setting 115
12.4.3 Group Address 116
13 Routing 117
13.1 IPv4 Management and Interfaces 117
13.1.1 IPv4 Interface 117
13.1.2 IPv4 Routes 118
13.1.3 ARP 119
13.2 IPv6 Management and Interfaces 120
13.2.1 IPv6 Interface 120
13.2.2 IPv6 Address 121
13.2.3 IPv6 Routes 122
13.2.4 Neighbors 123
14 Security 124
14.1 RADIUS 124
14.2 TACACS+ 125
14.3 AAA 127
14.3.1 Method List 127
14.3.2 Login Authentication 128
14.4 Management Access 128
14.4.1 Management VLAN 128
14.4.2 Management Service 129

14.4.3 Management ACL 130
14.5 Authentication Manager 132
14.5.1 Property 132
14.5.2 Port Setting 134
14.5.3 MAC-Based Local Account 135
14.5.4 WEB-Based Local Account 135
14.5.5 Sessions 136
14.6 DoS 136
14.6.1 Property 136
14.6.2 Port Setting 137
14.7 Dynamic ARP Inspection 138
14.7.1 Property 138
14.7.2 Statistics 139
14.8 DHCP Snooping 139
14.8.1 Property 140
14.8.2 Statistics 142
14.8.3 Option82 Property 142
14.9 IP Source Guard 147
14.9.1 Port Setting 148
14.9.2 IMPV Binding 149
15 ACL 150
15.1 MAC ACL 151
15.2 IPv4 ACL 153
15.3 IPv6 ACL 155
15.4 ACL Binding 158
16 QoS 159
16.1 General 161
16.1.1 Property 161
16.1.2 Queue Scheduling 162
16.1.3 CoS Mapping 164

16.1.4 DSCP Mapping 165
16.1.5 IP Precedence Mapping 166
16.2 Rate limit 167
16.2.1 Ingress / Egress Port 167
16.2.2 Egress Queue 168
17 Diagnostics 169
17.1 Logging 169
17.2 Ping 170
17.3 Traceroute 171
17.4 Copper Test 172
17.5 Fiber Module 172
17.6 UDLD 173
17.6.1 Property 173
17.6.2 Neighbor 174
18 Management 175
18.1 User Account 175
18.2 Firmware 176
18.3 Configuration 176
18.3.1 Upgrade 176
18.3.2 Save Configuration 177
18.4 SNMP 178
18.4.1 View 180
18.4.2 Group 180
18.4.3 Community 181
18.4.4 User 182
18.4.5 Engine ID 183
18.4.6 Trap Event 184
18.4.7 Notification 184
18.5 RMON 185
18.5.1 Statistics 186

18.5.2 History 187
18.5.3 Event 188
18.5.4 Alarm 190

1 소개 및 설치

1.1 제품 주요 사양

General Performance Indicator	
Product Model	MR-800K Series
Interface	8×10/100/1000M PoE Ports + 2×Gigabit SFP Ports + 1×Console Port
Poe Parameters	PoE Standard: IEEE802.3at(30W) and IEEE802.3af(15.4W)
	PoE compatibility: IEEE 802.3af/at adaptive
Physical Dimension	Product size: 172×155×55mm
	Product weight: 1.1kg
Working Environment	Operating Temperature: -40 ~ 85°C
	Storage Temperature: -40 ~ 85°C
	Operating Humidity: Max 95%, non-condensing
Technical Indicators	
Bandwidth	20Gbps
Packet Forwarding rate	14.88Mpps
Flash Capacity	128M
Memory Capacity	1024M

MAC	8K
Layer 2 Software Function	
Port Management	Enable/Disable Port, Speed, Duplex, MTU Setting Flow-control , Port information view
Port Mirroring	Support port mirroring
Port Speed Limit	Support port speed limit
Port Isolation	Support port isolation settings
Storm Suppression	Support unknown unicast, multicast, broadcast type storm suppression
Link Aggregation	Support static manual aggregation and LACP dynamic aggregation
VLAN	Support VLAN and IEEE 802.1Q VLAN
MAC	Support static addition, deletion
Spanning Tree	STP, RSTP, MSTP
Extended Function	
ACL	Based on MAC, IP, protocol type, L4 port
QoS	Based on 802.1p(COS) and DSCP classification(MR-800K-S only)
LLDP	Support LLDP link discovery protocol
User Setting	Add/delete users
Certification	Support 802.1x port authentication and AAA certification
Network diagnosis	Support ping, telnet, trace

System management	Device reset, configuration save/restore, upgrade management
Management Function	
CLI	Support serial port command line management
SSH	Support SSHv1/2 remote management
Telnet	Support telnet remote management
Web	Support Layer2 settings, Layer2 and Layer3 monitor
SNMP	SNMP V1/V2/V3
Other functions	TACACS+ and RADIUS Certification(MR-800K-S only)

1.2 제품 구성품

▶ MR-800K Switch × 1 대

▶ 제품 사양서 × 1 개

1.3 제품 외관

▶ 제품 전면부



▶ LED 동작상태

PWR	Lighting: Powered Un-Light: No Power
SYS	Flashing: System Start-up Lighting: System Running
PoE (1-8Port)	Lighting: Powered Un-Light: No Power
Link/ACT (1-8Port)	Lighting: Connected Flashing: Data transmission Un-Light: Not connected
9-10	Lighting: Connected Flashing: Data transmission Un-Light: Not connected

1.4 제품 설치

▶ 제품 설치 방법

1. 제품에 부착되어 있는 DIN-Rail 마운트 브라켓을 이용하여 DIN-Rail 에 설치합니다. 본 제품은 Fanless 제품으로 설치 시 통풍에 유의하십시오.

2. DC 전원(48-55V)을 연결하고, 제품 전면부의 PWR 와 SYS LED 점등을 확인합니다. 웹 UI 또는 콘솔 포트를 이용해 제품이 정상 동작하는지 확인합니다.

3. SFP 모듈(GBIC)을 사용할 경우 9~10 번 포트에 장착합니다.

4. TP 포트 또는 SFP 포트에 케이블을 이용하여 네트워크 디바이스를 연결합니다. PoE 장치를 연결할 경우 본 제품에서 PoE 기능이 포트별로 자동 활성화 됩니다.

5. TP 포트 또는 SFP 포트에 케이블을 이용하여 네트워크 디바이스를 연결합니다. PoE 장치를 연결할 경우 본 제품에서 PoE 기능이 자동으로 활성화 됩니다.

1.5 안전을 위한 주의사항

▶ 주의 사항

1. 정격 전원 이상의 콘센트를 단독으로 사용하지 마십시오. 또한 전원 코드를 임의로 연장하지 마십시오.

2. 열원 근처나 습기, 기름, 먼지가 많은 곳, 직사광선 및 물이 닿는 곳 등에 설치하지 마십시오.

3. 전원 플러그를 뺄 때에는 전원 코드 전선 부분을 당기지 마시고, 전원 플러그를 잡고 빼 주십시오.

4. 전원 코드를 무리하게 구부리거나, 묶지 마십시오.

5. 전원 인가된 제품 또는 전원 플러그를 젖은 손으로 만지지 마십시오.

6. 임의로 분해 또는 수리하지 마십시오.

2 Web Page Login

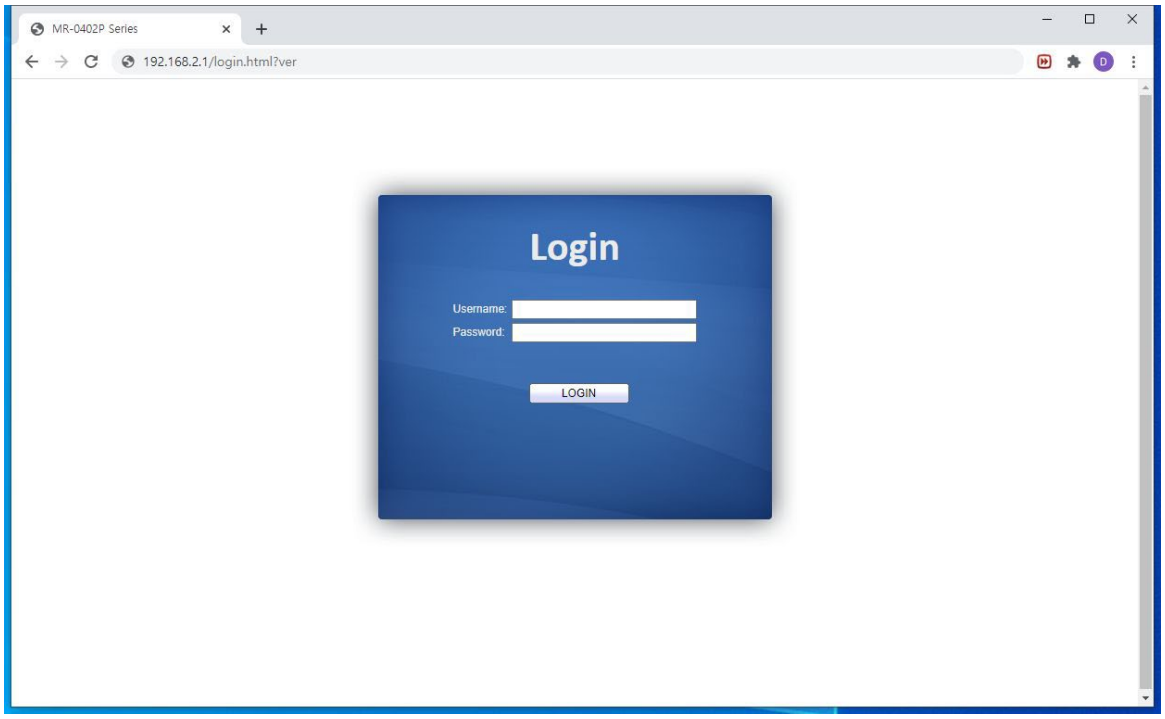
2.1 네트워크 관리 클라이언트에 로그인

기본 스위치 주소 : http://192.168.11.10 을 입력하고 "Enter"를 누릅니다.

Description:

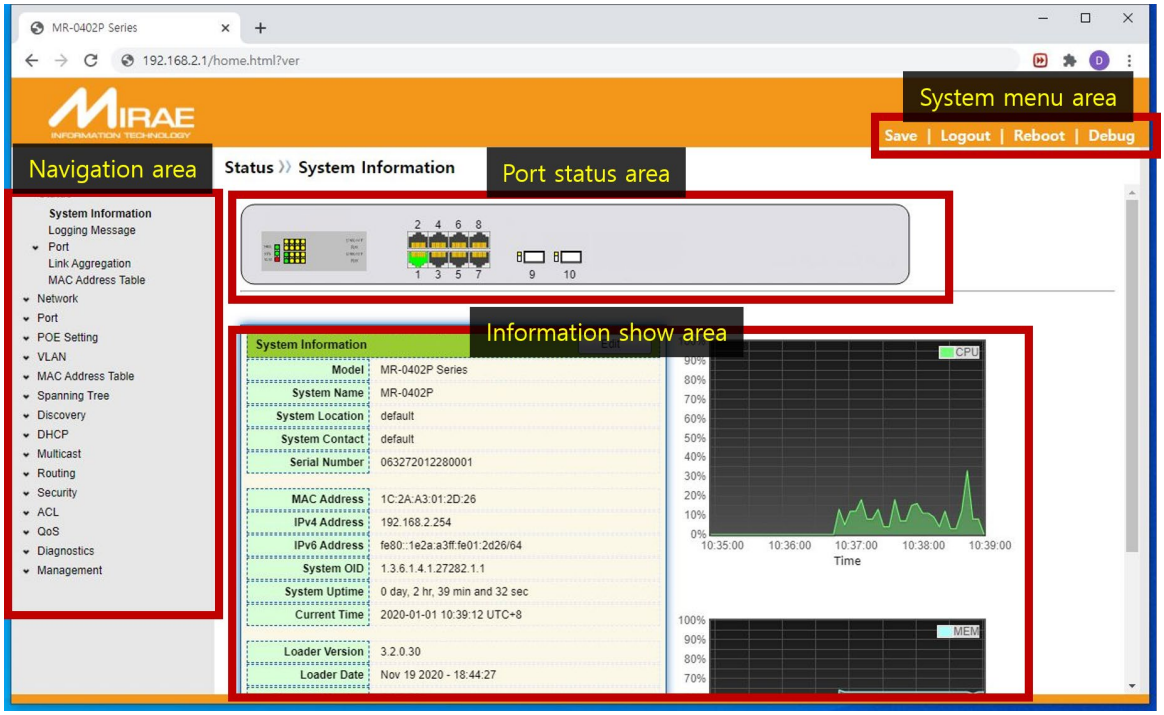
브라우저 표준 : IE 8.0, Chrome 23.0 및 Firefox 20.0 이상.
PC 의 IP 네트워크 세그먼트를 스위치의 IP 네트워크 세그먼트와 동일하게 유지하되 로그인 할 때 IP 주소를 구분하십시오. 첫 번째 로그인에 대해 PC 의 IP 주소를 192.168.11.x 로 설정하고 서브넷 마스크를 255.255.255.0 으로 설정하십시오 (1 <x ≤254).

다음과 같은 로그인 창이 나타납니다. 기본 사용자 이름 "admin"과 암호 "admin"을 입력합니다. 스위치 시스템을 보려면 "로그인"을 클릭하십시오.



2.2 클라이언트 인터페이스 구성

웹 네트워크 관리 시스템의 일반적인 운영 인터페이스는 다음과 같습니다.



2.3 웹 인터페이스의 탐색 트리

시스템 상태, 네트워크 구성, 포트, PoE 설정, VLAN 기능, MAC 주소 테이블, STP, 토폴로지 검색, 멀티 캐스트, 보안, ACL, QoS, 장치 진단 및 관리와 같은 메뉴 항목은 웹 네트워크 관리 클라이언트에서 사용할 수 있습니다. 각 항목에는 하위 메뉴가 있습니다. 탐색 트리는 다음과 같이 자세히 설명됩니다:

메뉴 항목	하위 메뉴	보조 하위 메뉴	설 명
Status	System Information		포트 상태 및 제품 정보 표시
	Logging Message		장치 실행 및 작동 로그 표시
	Port	Statistics	자세한 포트 통계 표시
		Error Disabled	포트에 발생한 오류 표시
		Bandwidth Utilization	모든 포트의 단위 시간당 대역폭 사용률 표시
	Link Aggregation		집계 그룹 상태 및 구성원 표시
	MAC Address Table		현재 장치의 **MAC** 주소 테이블 표시
Network	IP Address		현재 장치의 관리 **IP** 구성 및 보기
	DNS		**DNS** 및 서버 설정 구성 및 보기

	Hosts		**DNS** 서버 및 동적 호스트 매핑 테이블 구성 및 보기
	System Time		현재 시스템 시간 구성 및 보기
Port	Port Setting		모든 포트 구성 및 보기
	Error Disabled		오류 보호 구성 및 보기
	Link Aggregation	Group	**LAG** 에 포함 된 포트 및 전략 밸런싱 알고리즘 구성 및 보기
		Port Setting	**LAG** 구성 및 보기
		LACP	**LACP** 시스템 우선 순위 및 포트 구성 확인
	EEE		**EEE** 상태 및 정보 구성 및 보기
	Jumbo Frame		시스템에서 전달하는 최대 메시지 길이 구성 및 보기
	Port Security		포트 상태 및 포트 보안의 속도 제한 구성 및 보기
	Protected Port		포트 격리 구성 및 보기
	Storm Control		포트 스톰 정책 구성 및 보기
	Mirroring		포트 미러링 구성 및 보기
POE Setting	PoE Port Setting		PoE 포트 구성 및 보기
	PoE Port Timer Setting		PoE 포트 타이머 구성 및 보기
	PoE Port Timer Reboot Setting		PoE 포트 재시작 스케줄 구성 및 보기
VLAN	VLAN	Create VLAN	장치의 **VLAN** 정보 구성 및 보기
		VLAN Configuration	모든 포트의 **VLAN** 구성 구성 및 보기
		Membership	**VLAN** 의 포트 정보 구성 및 보기
		Port Setting	포트의 **PVID** 및 **VLAN** 속성 구성 및 보기
	Voice VLAN	Property	기능 스위치 및 포트 상태 구성 및 보기
		Voice OUI	**OUI** 성능 구성 및 보기
	Protocol VLAN	Protocol Group	프로토콜 **VLAN** 그룹 구성 및 보기
		Group Binding	프로토콜 **VLAN** 포트 및 그룹 바인딩을 구성하고 봅니다.
	MAC VLAN	MAC Group	**MAC VLAN** 그룹 구성 및 보기

		Group Binding	**MAC VLAN** 포트 및 그룹 바인딩 구성 및 보기
	Surveillance VLAN	Property	Surveillance-VLAN 기능 및 포트 상태 정보 구성 및 보기
		Surveillance OUI	Surveillance-VLAN OUI 정보 구성 및 보기
	GVRP	Property	기능 시스템 및 포트 상태 구성 및 보기
		Membership	학습 된 **VLAN** 및 포트 구성원 구성 및 보기
		Statistics	포트와 관련된 메시지 통계 구성 및 보기
MAC Address Table	Dynamic Address		장치의 동적 **MAC** 주소 및 노화 시간 구성 및 보기
	Static Address		장치의 정적 **MAC** 주소 테이블 구성 및 보기
	Filtering Address		필터링 할 **MAC** 주소 테이블 구성 및 보기
	Port Security Address		포트 보안에 의해 학습 된 **MAC** 주소 테이블 구성 및 보기
Spanning Tree	Property		STP 상태 및 속성 구성 및 보기
	Port Setting		STP 의 포트 속성 구성 및 보기
	MST Instance		STP 의 인스턴스 속성 구성 및 보기
	MST Port Setting		STP 의 인스턴스 (포트 정보 포함) 구성 및 보기
	Statistics		각 포트의 STP 메시지 통계 구성 및 보기
Discovery	LLDP	Property	LLDP 와 관련된 속성 구성 및 보기
		Port Setting	각 포트에서 LLDP 의 송수신 상태 구성 및 보기
		MED Network Policy	MED 네트워크 전략 테이블 항목 구성 및 보기
		MED Port Setting	각 포트에서 MED 상태 구성 및 보기
		Packet View	각 포트에서 자세한 LLDP 메시지 구성 및 보기
		Local Information	LLDP 및 LLDP-MED 상태 구성 및 보기
		Neighbor	LLDP 이웃 정보 구성 및 보기

		Statistics	각 포트에서 LLDP 메시지 송수신 상태 구성 및 보기
DHCP	Property		DHCP 서비스 구성 및 보기
	IP Pool Setting		DHCP 서버 IP 주소 pool 구성 및 보기
	VLAN IF Address Group Setting		VLANIF 및 DHCP 서버 그룹 구성 및 보기
	Client List		DHCP 클라이언트 목록 보기
	Client Static Binding Table		DHCP 클라이언트 정적 바인딩 테이블 구성 및 보기
Multicast	General	Property	기능 구성 구성 및 보기
		Group Address	관련 정적 멀티 캐스트 정보 구성 및 보기
		Router Port	멀티 캐스트 라우팅 포트 정보 구성 및 보기
		Forwarding All	멀티 캐스트 전달 포트 정보 구성 및 보기
		Throttling	각 포트에서 멀티 캐스트 제한 구성 및 보기
		Filtering Profile	필터링 된 멀티 캐스트 주소 구성 및 보기
		Filtering Binding	필터링 규칙 및 포트와 관련된 바인딩 정보 구성 및 보기
	IGMP Snooping	Property	스위치, 버전 등을 구성하고 확인합니다.
		Querier	쿼리 기 상태 구성 및 보기
		Statistics	프로토콜 메시지 구성 및 보기
	MLD Snooping	Property	프로토콜, 스위치 등을 구성하고 보기
		Statistics	프로토콜 메시지 구성 및 보기
	MVR	Property	스위치와 같은 속성 정보 구성 및 보기
		Port Setting	각 포트에서 상태 구성 및 보기
		Group Address	기능, VLAN 및 그룹 주소 구성 및 보기
Routing	IPv4 Management and Interfaces	IPv4 Interface	Configure and view VLANIF IPv4 address information
		IPv4 Routes	Configure and view IPv4 static routes

		ARP	Configure and view ARP table
	IPv6 Management and Interfaces	IPv6 Interface	Configure and view VLANIF IPv6 interface information
		IPv6 Address	Configure and view VLANIF IPv6 address information
		IPv6 Routes	Configure and view IPv6 static routes
		IPv6 Neighbors	Configure and view IPv6 neighbors table
Security	RADIUS		서버와 관련된 정보 구성 및 보기
	TACACS+		서버와 관련된 정보 구성 및 보기
	AAA	Method List	로그인 인증 방법 구성 및 보기
		Login Authentication	단말기의 인증 방법 구성 및 보기
	Management Access	Management VLAN	현재 VLAN 관리 정보 구성 및 보기
		Management Service	서비스 관리 모드 및 관련 속성 구성 및 보기
		Management ACL	관리 채널을 겨냥한 ACL 구성 및 보기
		Management ACE	관리 채널의 ACE 구성 구성 및 보기
	Authentication Management	Property	인증 속성 구성 및 보기
		Port Setting	각 포트에서 인증 정보 구성 및 보기
		MAC Local Account	MAC 로컬 계정 목록 구성 및 보기
		Web Local Account	웹 로컬 계정 목록 구성 및 보기
		Sessions	세션 인증과 관련된 정보 구성 및 보기
	DoS	Property	스위치 옵션 구성 및 보기
		Port Setting	포트에서 스위치 옵션 구성 및 보기
	Dynamic ARP Inspection	Property	동적 ARP 검사 구성 및 보기
		Statistics	각 포트에서 APR 검사 상태의 메시지 통계 구성 및 보기
	DHCP Snooping	Property	스위치 및 상태 구성 및 보기
		Statistics	각 포트에서 수신 한 DHCP 메시지 통계 구성 및 보기
		Option82 Property	옵션 82 와 관련된 속성 구성 및

			보기
		Option82 Circuit ID	옵션 82 의 회로 ID 구성 및 보기
	IP Source Guard	Port Setting	포트에서 상태 구성 및 보기
		IMPV Binding	IP, MAC, 포트 및 VLAN 의 바인딩 테이블 구성 및 보기
		Save Database	바인딩 테이블 항목의 저장소 및 정보 구성 및 보기
ACL	MAC ACL		MAC ACL 규칙 구성 및 보기
	MAC ACE		MAC ACE 테이블 항목 구성 및 보기
	IPv4 ACL		IPv4 ACL 규칙 구성 및 보기
	IPv4 ACE		IPv4 ACE 테이블 항목 구성 및 보기
	IPv6 ACL		IPv6 ACL 규칙 구성 및 보기
	IPv6 ACE		IPv6 ACE 테이블 항목 구성 및 보기
	ACL Binding		ACL 규칙 및 포트 바인딩 애플리케이션 구성 및 보기
QoS	General	Property	QoS 스위치 및 상태 구성 및 보기
		Queue Scheduling	대기열 예약 알고리즘 구성 및 보기
		CoS Mapping	우선 순위 및 로컬 대기열 매핑 테이블 구성 및 보기
		DSCP Mapping	우선 순위 및 로컬 대기열 매핑 테이블 구성 및 보기
		IP Precedence Mapping	우선 순위 및 로컬 대기열 매핑 테이블 구성 및 보기
	Rate Limit	Ingress/Egress Port	포트 속도 제한 구성 및 보기
		Egress Queue	송신 대기열을 기반으로 속도 제한 구성 및 보기
Diagnostics	Logging	Property	스위치 및 상태 구성 및 보기
		Remote Server	원격 서버의 주소 구성 및 보기
	Ping		Ping 에 의한 네트워크 진단
	Traceroute		Traceroute 에 의한 네트워크 진단
	Copper Test		VCT 에 의한 전기 인터페이스 링크 진단
	Fiber Module		광학 인터페이스에서 SFP 모듈

			확인
	UDLD	Property	스위치 및 상태 구성 및 보기
		Neighbor	인접 상태 구성 및 보기
Management	User Account		사용자 정보 구성 및 보기
	Firmware	Upgrade	소프트웨어 업데이트
	Configuration	Upgrade	구성 파일 업데이트
		Save Configuration	실행중인 장치를 지원하는 구성 파일을 저장합니다
	SNMP	View	SNMP 기능보기 테이블 항목 구성 및 보기
		Group	SNMP 그룹 구성 및 보기
		Community	SNMP 커뮤니티 구성 및 보기
		User	SNMP 사용자 속성 구성 및 보기
		Engine ID	SNMP 및 원격 엔진 ID 구성 및 보기
		Trap Event	SNMP 트랩 스위치 및 상태 구성 및 보기
		Notification	SNMP 알림 서버 상태 구성 및 보기
	RMON	Statistics	모든 포트의 메시지 통계 기록 구성 및 보기
		History	내역 기록 상태 구성 및 보기
		Event	이벤트 상태 구성 및 보기
		Alarm	경보 상태 구성 및 보기

3 Status

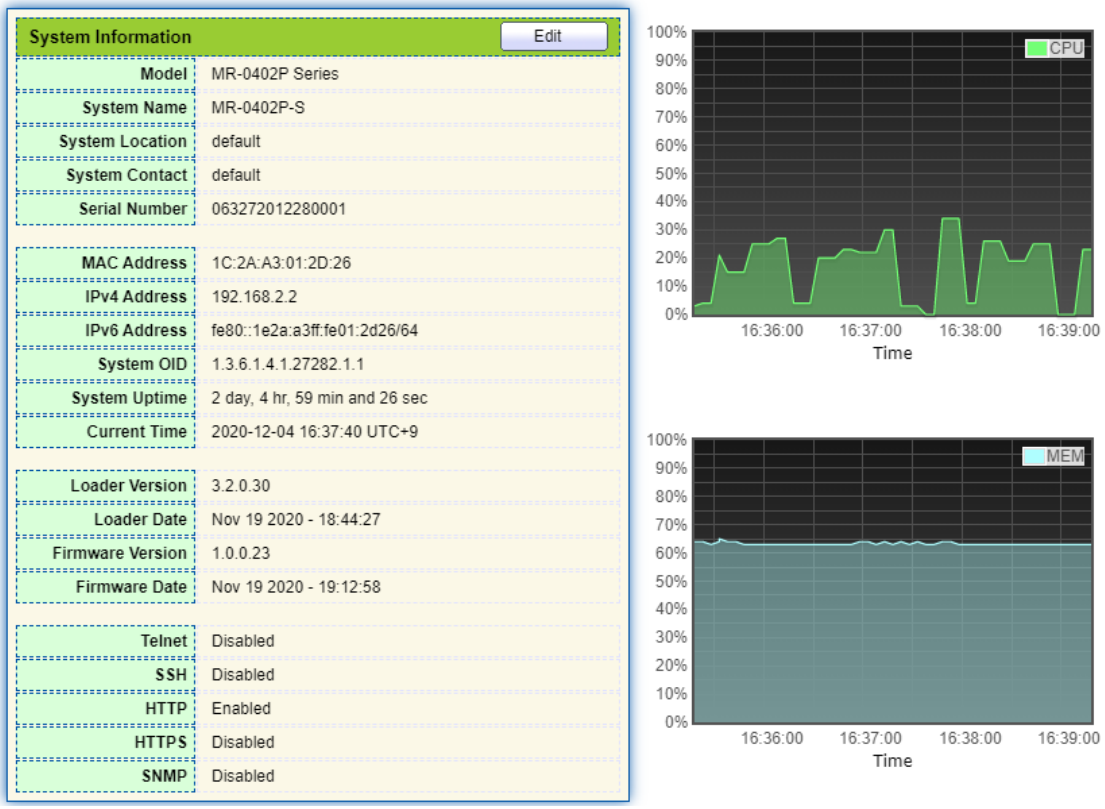
3.1 System Information

연결된 스위치에 따라 웹 네트워크 관리 패널은 포트 수, 포트 상태, 제품 정보, 장치 상태, 기능 켜기 / 끄기 상태 등을 포함하여 포트 및 제품 정보를 직접 표시합니다.

Instructions:

1. 다음과 같이 탐색 트리에서 “Status > System Information”를 클릭합니다:





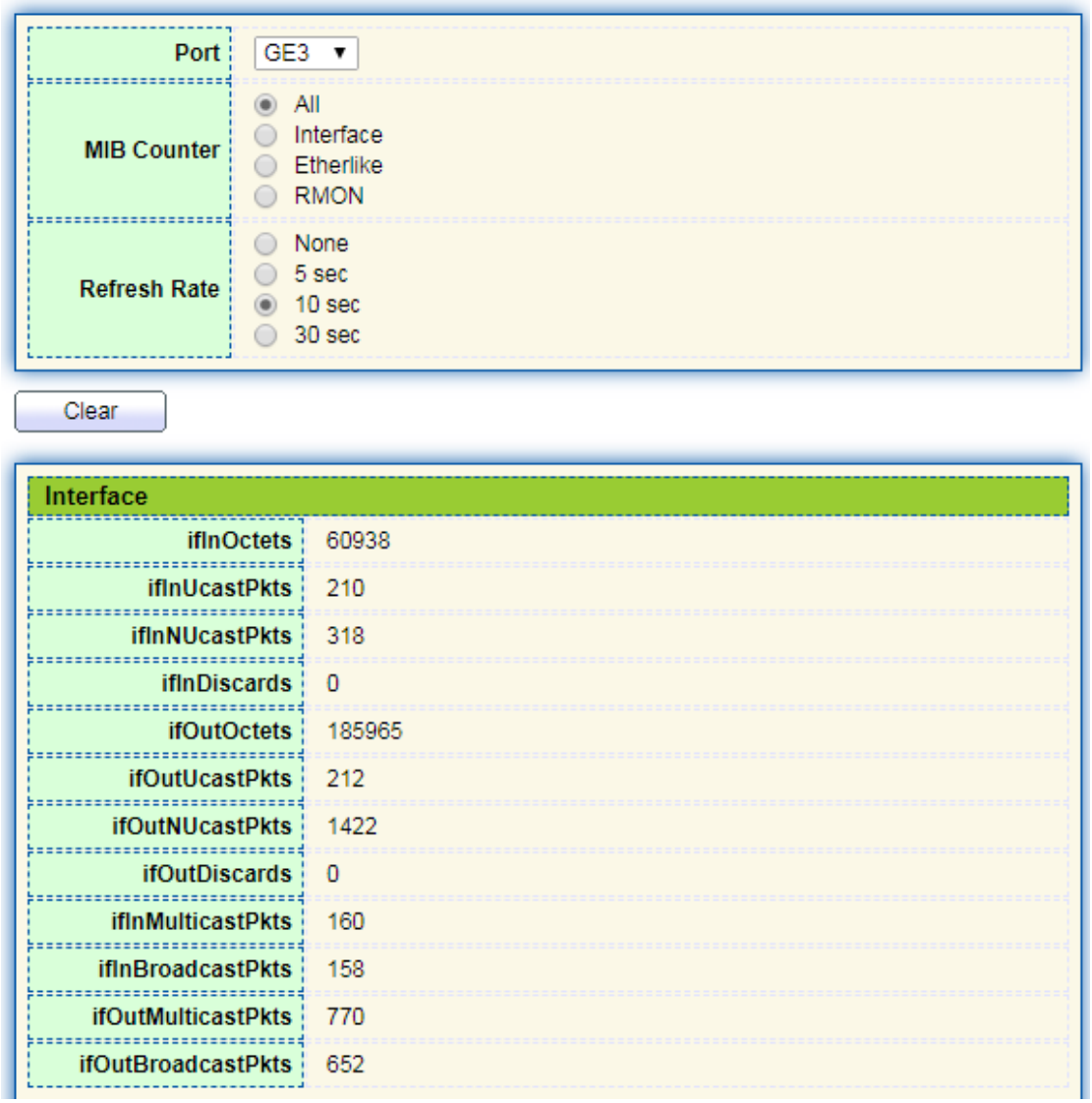
Description:

포트 번호, 유형, 속도 및 상태를 확인하려면 포트 위로 마우스를 가져갑니다.
제품 정보에서 “System Name”, “Location” 및 “Contact” 를 수정합니다. “Apply” 해서 완료합니다.

3.2 Statistics

포트의 자세한 흐름 통계 및 사용자가 수동으로 새로 고치거나 지울 정보에 대해 소개합니다.

1. 다음과 같이 탐색 트리에서 “Status > Port > Statistics”를 클릭합니다:



Description:

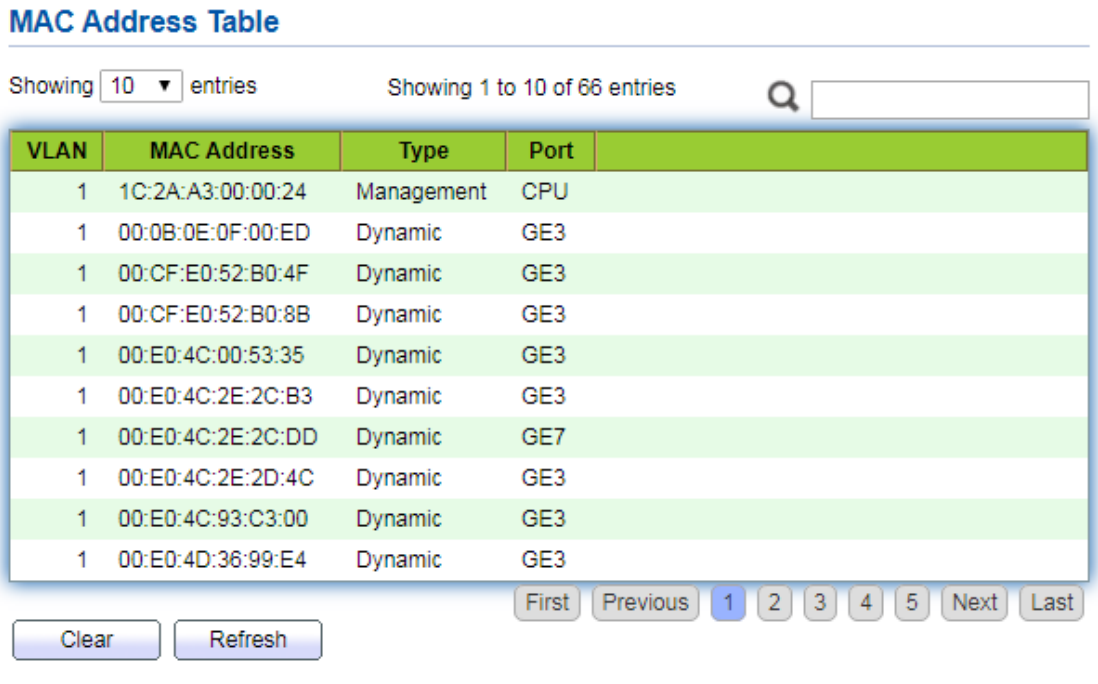
“Clear”는 현재 포트의 흐름 통계 및 페이지를 초기화하고 새로고침 합니다.

3.3 MAC Address Table

MAC address table 정보를 확인합니다.

Instructions:

1. 다음과 같이 탐색 트리에서 “Status > MAC Address Table”를 클릭합니다:



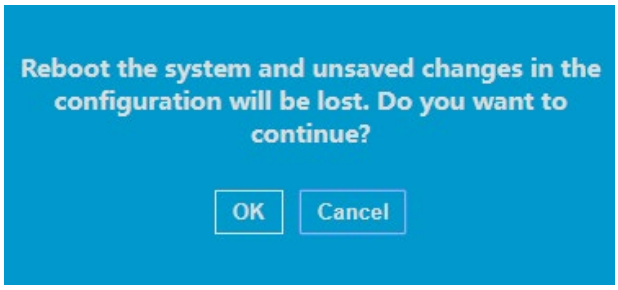
인터페이스 데이터는 다음과 같습니다.

항목	설명
MAC	목적지 MAC Address
VLAN	MAC address 에 속한 VLAN ID
Port	MAC address 에 해당하는 Port
Type	Dynamic MAC Address 는 설정된 에이징 시간에 따라 에이징되는 항목을 나타냅니다. 스위치는 MAC Address 또는 수동 생성의 학습 메커니즘을 기반으로 항목을 추가 할 수 있습니다. Static MAC Address 는 수동으로 구성되고 에이징되지 않는 지정된 테이블을 나타냅니다. Management MAC Address 는 관리 포트의 주소를 나타냅니다.

3.4 Reboot

1. 우측 상단의 “Reboot”를 클릭합니다.





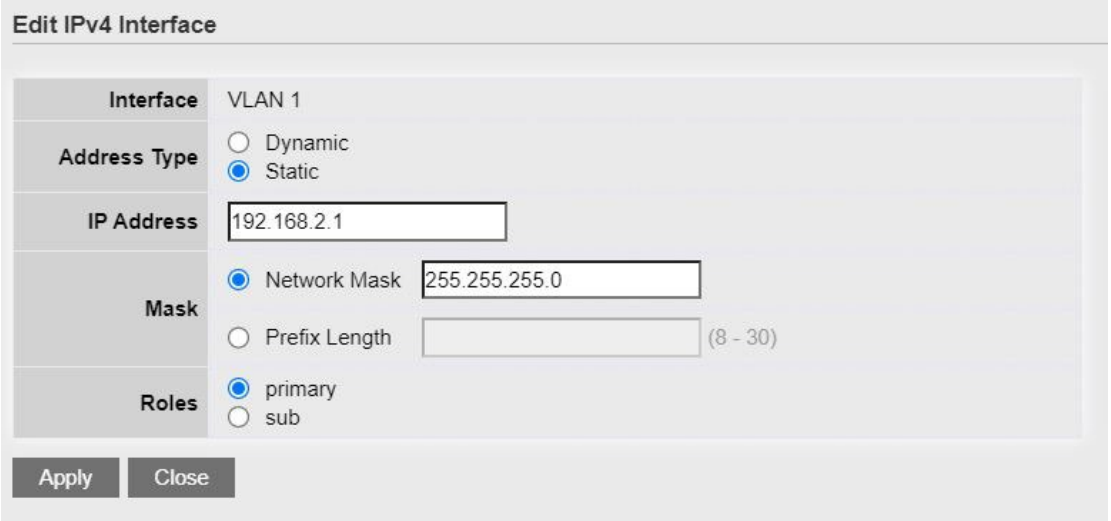
4 Network

4.1 IP Address

웹 인터페이스에서 관리 IP 주소를 변경합니다..

Instructions:

1. 탐색 모음에서 " Routing > IPv4 Management and Interfaces > IPv4 Interface "을 클릭합니다.
2. 변경을 원하는 VLAN 의 인터페이스를 선택한 다음 Edit 를 클릭합니다.
3. 수동 IP 를 입력할 경우, Address Type 을 Static 으로 설정한 다음, IP 주소와 netmask, role 을 설정합니다.
4. Apply 를 클릭해서 수정을 적용/완료합니다.



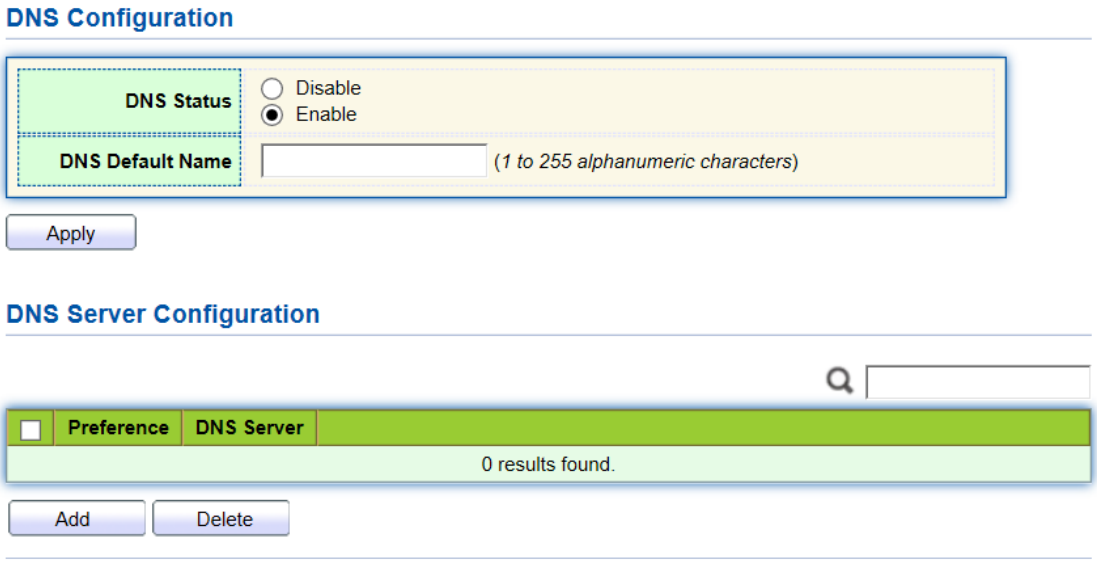
4.2 DNS

DNS 는 장치에서 도메인 계층으로 컴퓨터 및 네트워크 서비스의 이름을 지정하는 Domain Name System 의 약자입니다. 도메인 이름은 각각 고유 한 IP 주소에 해당하는 일련의 단어 또는 약어로 구분 된 점으로 구성됩니다. DNS 는 도메인 이름을 확인하는 인터넷 서버입니다. 인터넷 및 기타 TCP / IP 네트워크에 적용 할 수있는

DNS 이름은 사용자에게 친숙한 이름을 통해 컴퓨터와 서비스를 검색합니다.
핵심 인터넷 서비스 중 하나 인 DNS 는 도메인 이름과 IP 주소를 상호 매핑하는 분산 데이터베이스입니다.

Instructions:

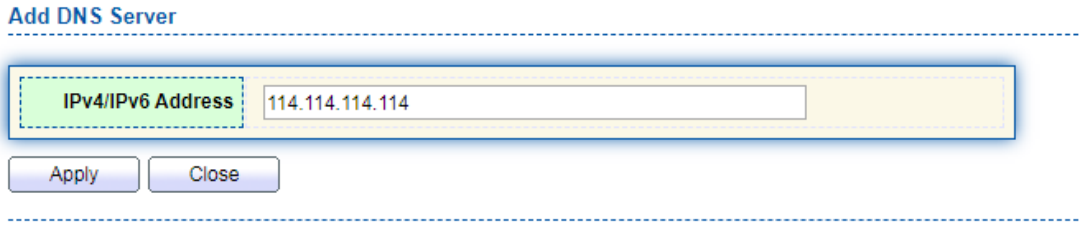
1. 다음과 같이 탐색 트리에서 “Network > DNS”를 클릭합니다.



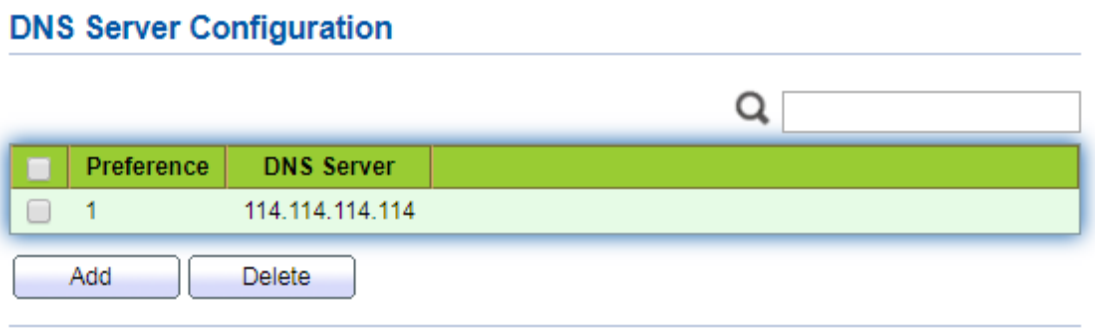
인터페이스 데이터는 다음과 같습니다.

구성 항목	설명
DNS State	DNS switch
DNS Default Name	DNS 의 기본 이름을 설정합니다.

2. DNS 서버를 구성하기 위해 “Add”를 클릭합니다.



3. “Apply”를 클릭하고 다음과 같이 마칩니다.



4.3 System Time

주로 시스템 시간을 구성하고 시간 소스, 일광 절약 시간 등을 선택하는 데 사용됩니다.

Instructions

1. 다음과 같이 탐색 트리에서 “Network > System Time”를 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

구성항목	설명
Time Source	**SNTP, PC** 또는 수동 모드에서 시간 소스 선택
Time Zone	시간대 설정
Address Type	호스트 이름 또는 **IPv4** 주소 **(SNTP** 에 의해 설정된 시간 원본 포함**)**
Server Address	서버 주소 **(SNTP** 에 의해 설정된 시간 소스 포함**)**
Server Port No.	서버 포트 번호 **(SNTP** 에 의해 설정된 시간 소스 포함**)**
Date	날짜 정보 **: dd / mm / yyyy** (시간 소스가 수동 모드로 설정된 경우**)**
Time	시간 정보 **: s / min / hr** (시간 소스가 수동 모드로 설정된 경우**)**
Type	일광 절약 시간 유형은 없음, 주기적, 비 주기적, 미국 및 유럽으로 구분됩니다.
Reimbursed Time	일광 절약 시간의 상환시간
Cyclic Mode	일광 절약 시간의 주기적 모드 구성
Non-cyclic Mode	일광 절약 시간의 비 주기적 모드 구성

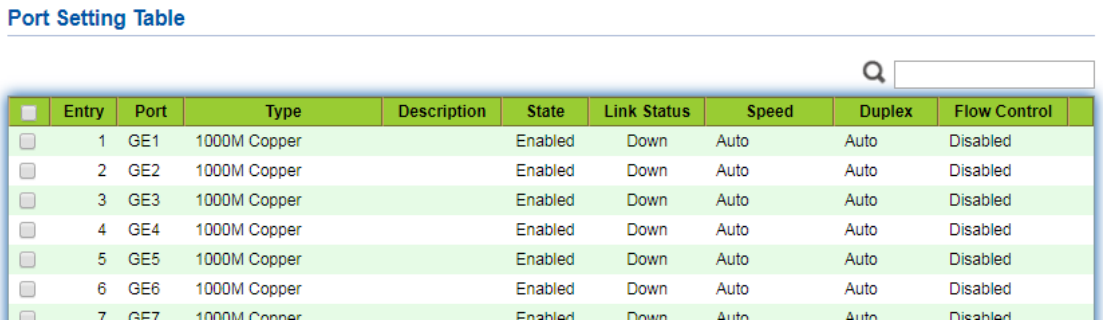
5 Port

5.1 Port Setting

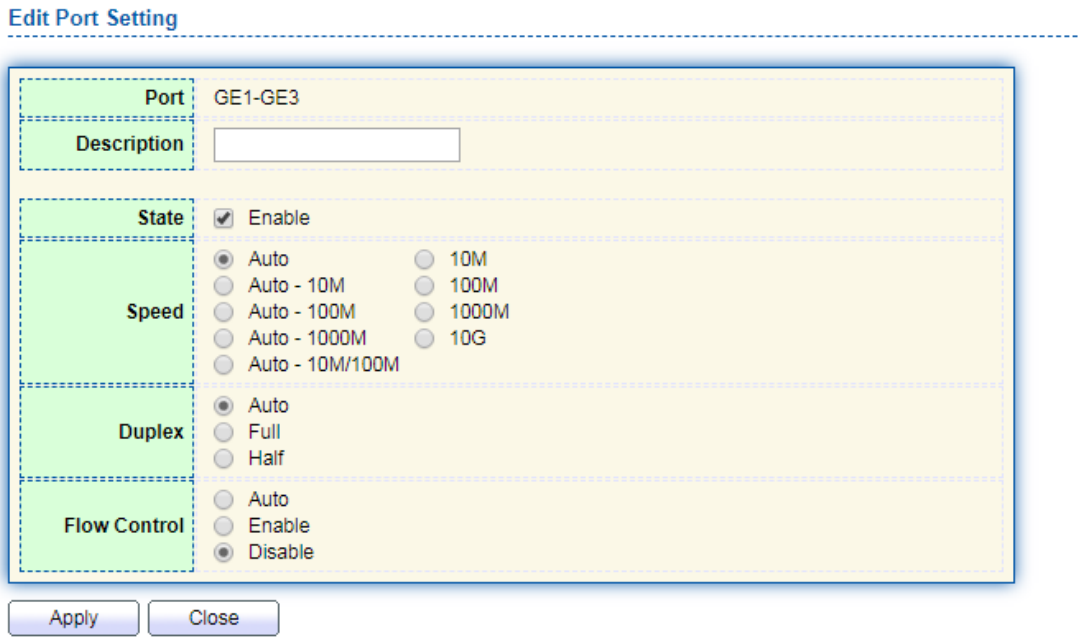
사용자가 원하는대로 이더넷 인터페이스를 조회하고 구성할 수 있도록 인터페이스를 식별해야합니다.

Instructions:

1. 다음과 같이 탐색 트리에서 “Port > Port Setting”를 클릭합니다:



2. 구성할 포트를 선택하고, “Edit”를 클릭합니다.



구성 항목은 다음과 같습니다.

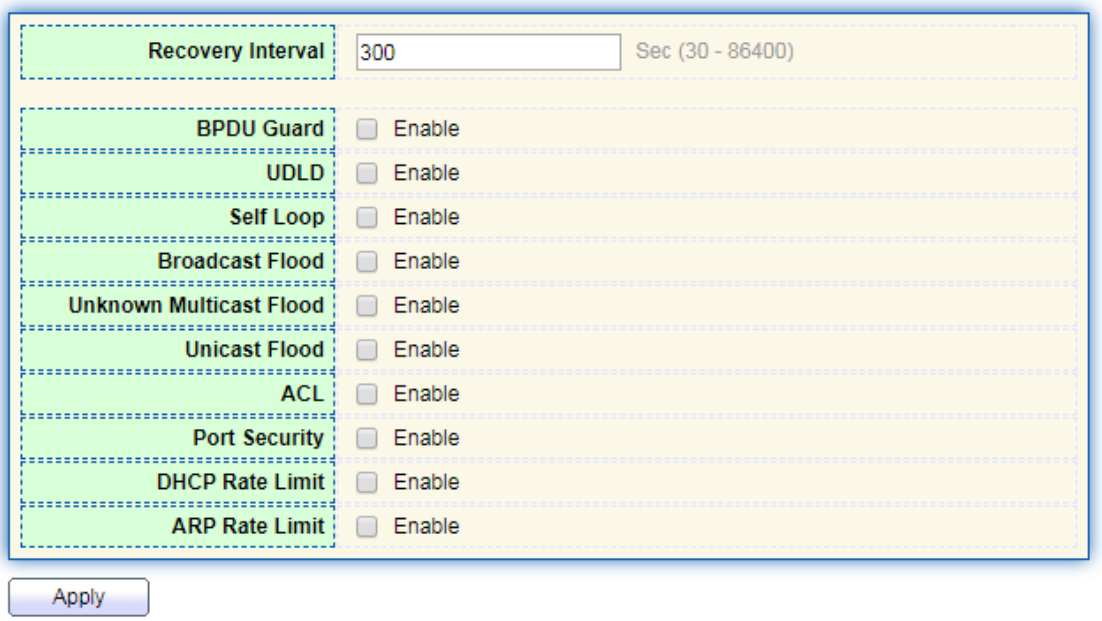
구성 항목	설명
Port	Port 리스트
Description	Port 설명
State	사용자는 필요에 따라 포트를 활성화 또는 비활성화 할 수 있습니다.
Speed	10Mb, 100Mb 및 1,000Mb 상태로 구성 가능한 자동 설정. 10Mbit / s, 100Mbit / s 및 1,000Mbit / s 를 포함한 인터페이스 속도는 이더넷 전기 인터페이스에 사용할 수 있으며 필요에 따라 선택 사항입니다.
Duplex	필수 전이중 또는 반이중으로 구성 가능한 자동 설정
Flow Control	로컬 네트워크와 반대쪽 네트워크 장치 모두에서 활성화되면 로컬 장치는 네트워크 정체가있는 경우 메시지 전송을 중지하도록 다른 장치에 알립니다. 반대쪽은 메시지 손실을 방지하기 위해 일시적으로 명령을 실행합니다. Disable-Disabled 수신 및 PAUSE 프레임 전송; PAUSE 프레임의 Enable-Enabled 수신 및 전송; 자동 설정-반대 네트워크 장치와 자동으로 PAUSE 프레임을 설정합니다.

5.2 Error Disabled

스위치가 포트에서 일부 오류를 감지하면 포트를 즉시 다운시키는 기능입니다.

Instructions:

1. 다음과 같이 탐색 트리에서 “Port > Error Disabled”를 클릭하여 기능을 활성화 또는 비활성화 합니다:



5.3 Link Aggregation

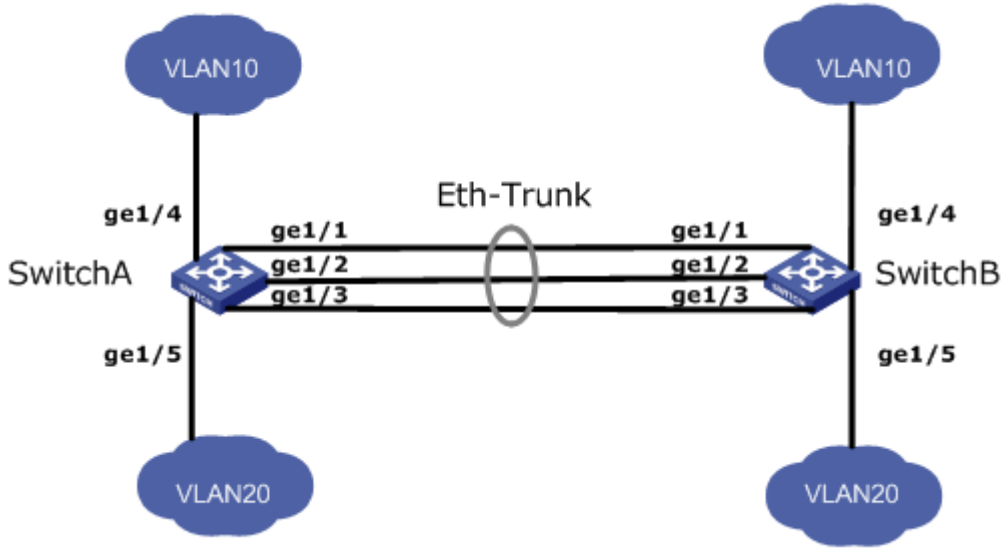
Link Aggregation 은 물리적 인터페이스 그룹을 단일 논리적 인터페이스로 묶어 대역폭과 안정성을 확장합니다.

LAG (Link Aggregation Group)는 여러 이더넷 링크 (Eth-Trunk)로 번들 된 논리적 링크입니다.

네트워크 크기를 끊임없이 확장하면 링크 대역폭과 안정성에 대한 사용자의 요구가 증가합니다. 전통적으로 고속 인터페이스 보드 또는 호환 장비는 일반적으로 대역폭을 최적화하기 위해 교체되며 비용이 많이 들고 유연성이 떨어집니다.

Link Aggregation Technology 는 하드웨어를 업그레이드하지 않고 여러 물리적 인터페이스를 단일 논리적 인터페이스로 묶습니다. 백업 메커니즘은 안정성을 향상시킬뿐만 아니라 다른 물리적 링크에서 흐름 부하를 공유합니다.

아래와 같이 스위치 A 는 Eth-Trunk 논리 링크에 번들로 제공되는 3 개의 이더넷 링크를 통해 스위치 B 와 연결됩니다. 대역폭은 총 3 개 링크의 대역폭과 동일하므로 대역폭이 넓어집니다. 한편, 이 세 링크는 서로 백업되어 더 안정적인 구성을 만듭니다.



Link Aggregation 은 다음 요구 사항을 충족 할 수 있습니다.

- 하나의 링크로 연결된 두 스위치의 대역폭이 충분하지 않다.
- 하나의 링크로 연결된 두 개의 스위치의 신뢰성이 부족하다.

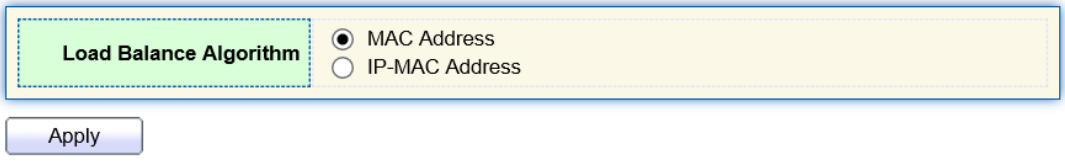
Link Aggregation 은 LACP (Link Aggregation Control Protocol) 상태에 따라 수동 모드와 LACP 모드로 나눌 수 있습니다.

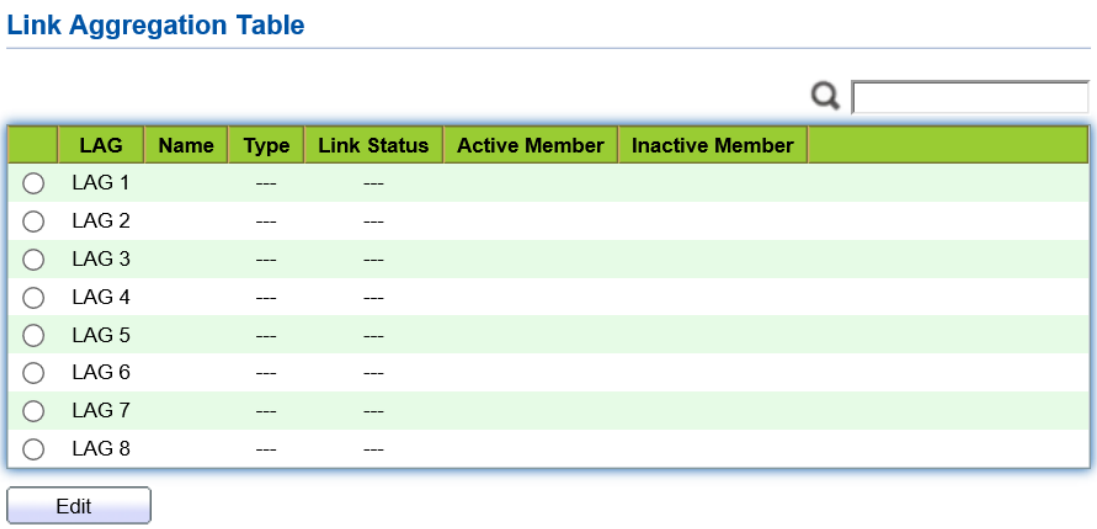
첫 번째 모드 인 Eth-Trunk 설정에서 멤버 인터페이스 액세스는 LACP 없이 수동으로 추가해야합니다. 모든 링크가 데이터 전달 및 로드 공유에 관련되기 때문에 로드공유모드라고도 합니다. 활성 링크가 실패하는 경우 LAG 는 나머지 링크와 함께 평균로드를 수행합니다. 이 모드는 직접 연결된 두 장치가 더 큰 링크 대역폭을 필요로하지만 LACP 에 액세스 할 수 없는 경우에 선호됩니다

5.3.1 Group

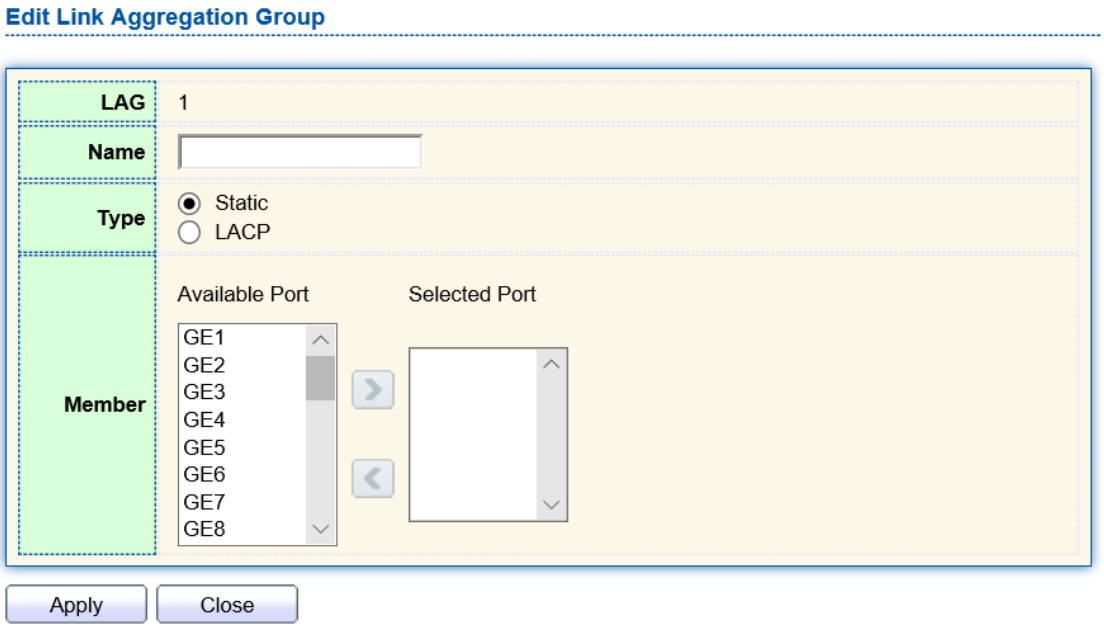
Static Link Aggregation 을 추가하는 방법:

1. “Port > Link Aggregation > Group” 을 클릭하고 라디오 버튼으로 로드 밸런싱 알고리즘을 선택합니다. 다음과 같이 “Apply” 하고 완료합니다:





2. 사용 가능한 **8** 개의 **LAG** 중 하나를 선택하고 다음과 같이 구성 페이지를 수정합니다:

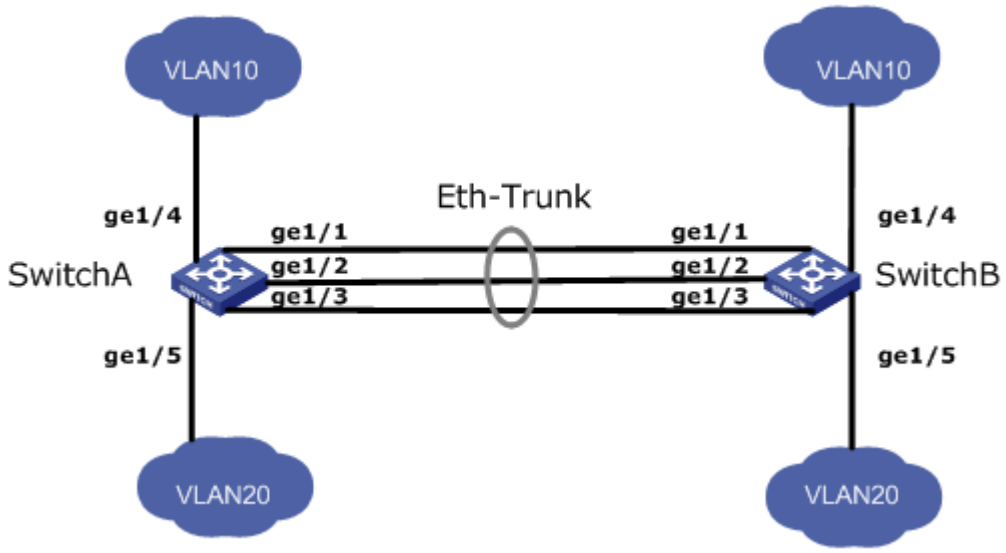


구성 항목은 다음과 같습니다.

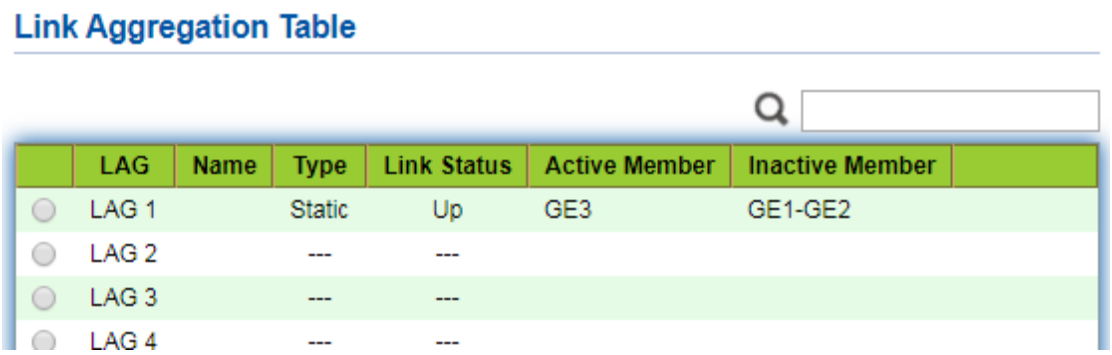
구성 항목	설명
LAG	**LAG 1** 에서 **8** 까지 번호가 매겨진 **8** 개의 **LAG** 가 있습니다.
Name	이름 필요에 따라 수정할 수있는 **LAG** 에 대한 설명입니다.
Type	모드 수동 모드와 **LACP** 모드에서 선택합니다.
Member	멤버 최대 **8** 개의 멤버 포트를 **LAG** 에서 사용할 수 있습니다.

Illustration:
아래에 표시된 것처럼 스위치 **A**와 스위치 **B**는 각각 이더넷을 통해 **VLAN 10**과 **20**을 연결하며 이들 사이에는 대용량 데이터 흐름이 있습니다.
스위치 **A** 와 **B** 는 모두 **VLAN** 통신을위한 우수한 링크 대역폭을 제공 할 것으로 예상됩니다. 한편, 안정적인 데이터 전송과 링크를위한 중복성이 있어야합니다.

수동 모드의 네트워킹 다이어그램 **LAG**



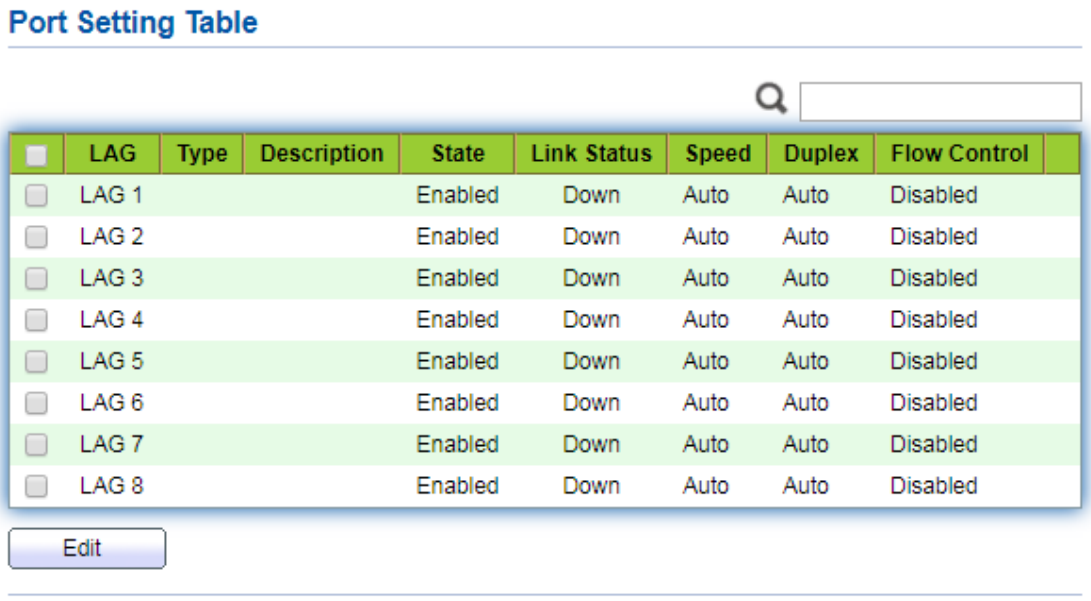
Instructions:
1. 스위치 **B** 구성 단계와 유사하게 스위치 **A** 는 **Eth-Trunk** 인터페이스를 생성하고 멤버 인터페이스에 액세스하여 링크 대역폭을 확장합니다. “Port > Link Aggregation > Group” 을 클릭하고 **"LAG 1"**과 포트 **GE1, 2** 및 **3** 을 선택한 다음 오른쪽에서 선택한 포트로 이동합니다. 다음과 같이 “Apply” 하고 완료합니다.



5.3.2 Port Setting

Aggregation group member port의 속성 구성

1. "Port > Link Aggregation > Port Setting"을 클릭하여 다음과 같이 Aggregation 그룹 멤버 포트의 속성 설정을 입력합니다:



5.3.3 LACP

IEEE 802.3ad 표준을 기반으로하는 **LACP (Link Aggregation Control Protocol)**는 링크를 동적으로 집계 및 분리합니다. **LACPDU (Link Aggregation Control Protocol Data Unit)**를 통해 반대 네트워크 장치와 정보를 교환합니다.

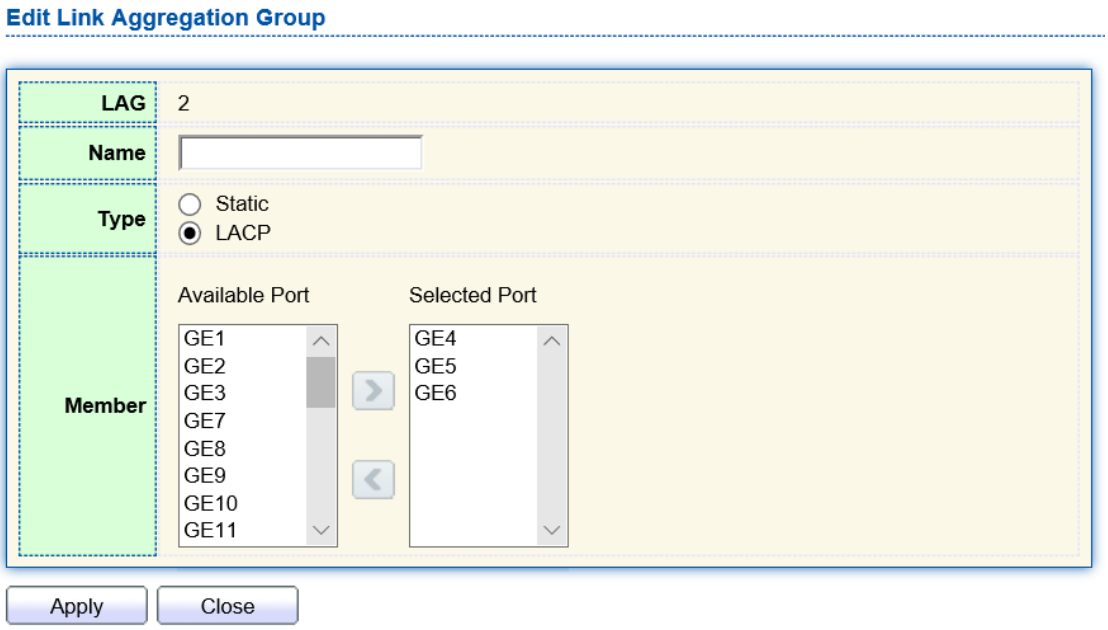
포트가 **LACP**를 사용하면 **LACPDU**를 전송하여 시스템 우선 순위, 시스템 **MAC**, 포트 우선 순위 및 번호, 작동 키를 상대 네트워크 장치에 알려줍니다. 반대 장치는 이러한 정보를 수신 한 후 다른 포트에서 저장 한 정보와 비교하여 동적 집계에 대한 포트 참여 또는 종료에 대한 동의에 도달합니다.

동적 **LACP** 집계는 시스템에 의해 자동으로 생성 또는 삭제됩니다. 즉, 내부 포트를

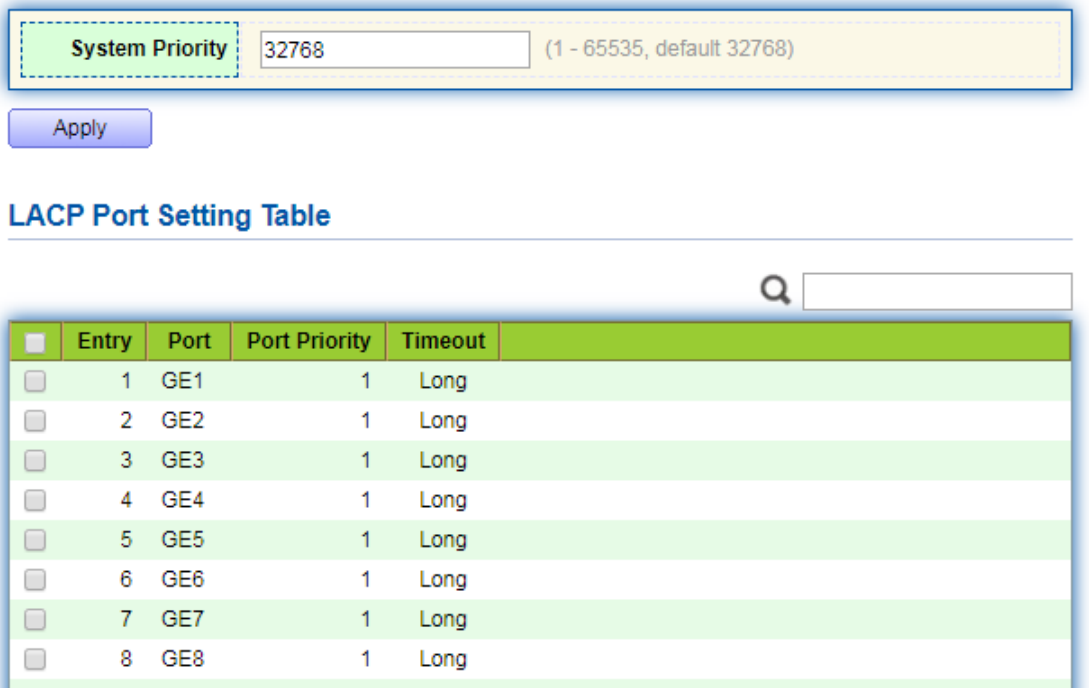
자체적으로 추가하거나 제거 할 수 있습니다. 동일한 속도, 이중 및 기본 구성으로 동일한 장치에 연결된 포트만 통합 할 수 있습니다.

Dynamic Link Aggregation 을 구성하기 위한 방법:

1. 탐색 트리에서 “Port > Link Aggregation > Group”을 클릭하고, LAG ID 를 선택한 다음, “Edit”를 클릭해서 다음과 같이 설정합니다:



2. 탐색 트리에서 “Port >Link Aggregation > LACP”을 클릭하여 다음과 같이 시스템 우선 순위, 포트 우선 순위 및 시간 초과와 같은 LACP 속성을 설정합니다:



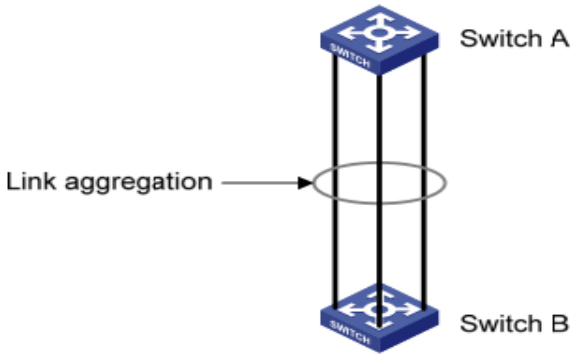
구성항목은 다음과 같습니다.

구성 항목	설명
System Priority	**LACP** 는 우선 순위 표준에 따라 두 장치 간의 활성 및 수동 모드를 결정합니다..
Port	Port 리스트
Port Priority	**LACP** 는 우수한 시스템의 포트 우선 순위에 따라 동적 **LAG** 멤버 모드를 결정합니다
Timeout	**LACP** 메시지의 전송 주파수를 결정합니다.

Description:

작업 패턴을 변경하기 전에 Eth-Trunk 에 액세스하는 멤버 인터페이스가 없는지 확인하십시오.
로컬 네트워크 장치의 작업 패턴은 반대 네트워크 장치의 작업 패턴과 일치해야합니다.

Illustration
이더넷 스위치 A 는 GE1 에서 GE3, 스위치 B 까지 3 개의 포트를 통합하여 각 멤버 포트별로 로드를 공유합니다.
다음 구성은 dynamic aggregation 을 통해 예시됩니다.

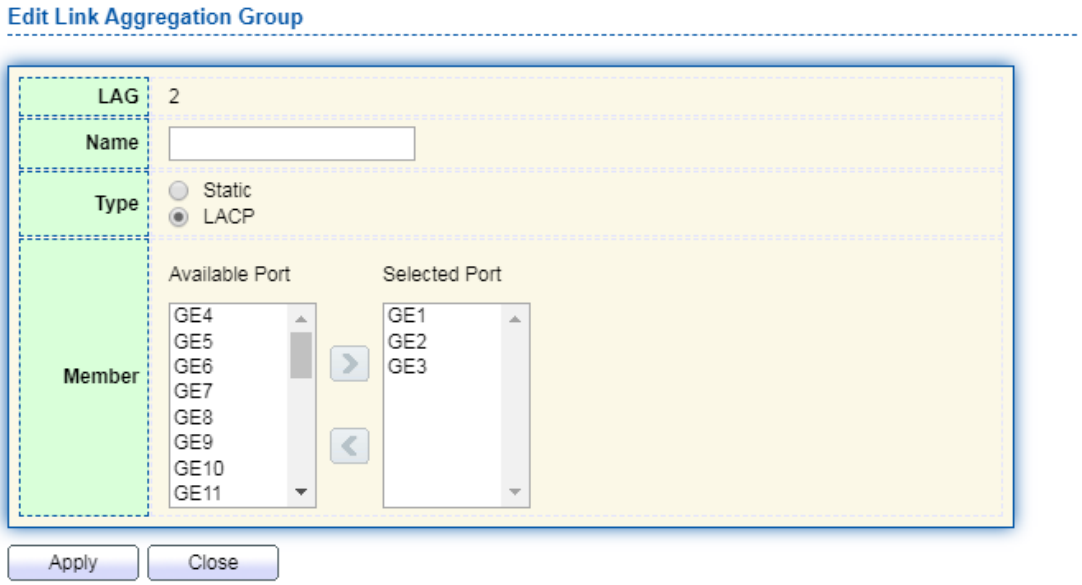


Description:

다음은 스위치 A 의 구성이며 포트 통합을 위해 스위치 B 의 구성과 동일해야합니다.

Instructions:

1. 탐색 트리에서 “Port > Link Aggregation > Group”을 클릭하고, LAG 2 를 선택한 뒤 “Edit”를 클릭합니다. GE1-GE3 를 LACP mode 로 설정하고, “Apply”를 클릭하여 마칩니다:

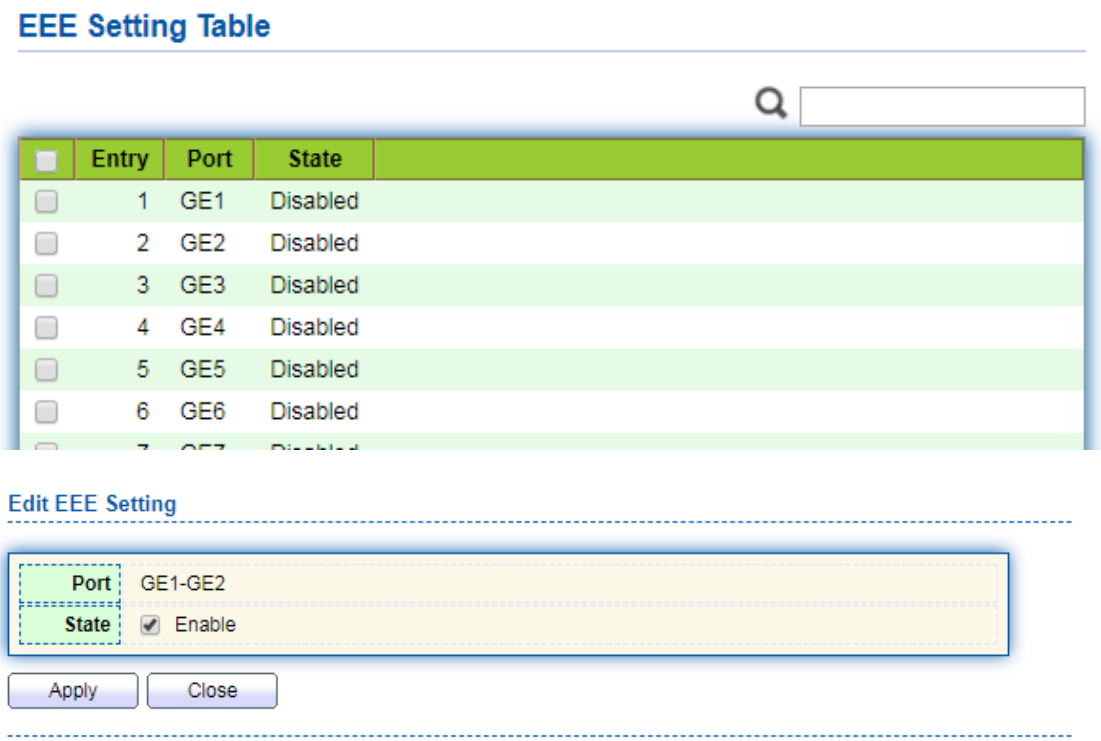


5.4 EEE

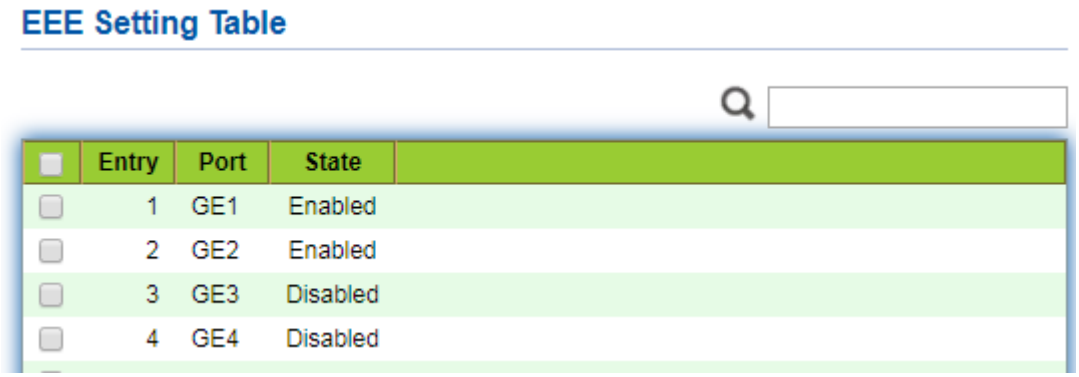
Flow 가 0 일 경우 포트 전원이 꺼집니다.

Instructions:

1. 탐색 트리에서 “Port > EEE”를 클릭하고, 포트를 선택한 뒤 “Edit”를 클릭합니다.:



2. 기능을 활성화 하고 “Apply”를 클릭하여 설정을 완료합니다:

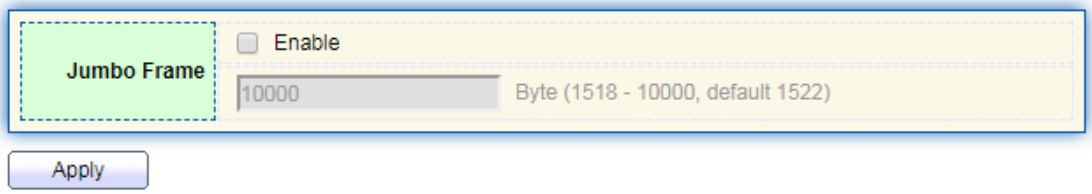


5.5 Jumbo Frame

포트의 MTU(Maximum Transmission Unit)를 설정합니다.

Instructions:

1. 탐색 트리의 “Port > Jumbo Frame”를 클릭하고, 다음과 같이 Jumbo Frame 설정을 합니다:

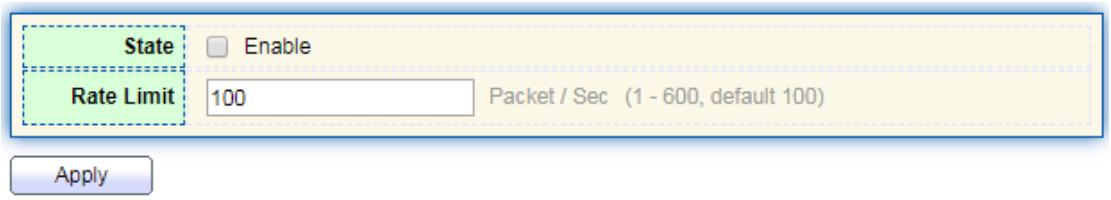


5.6 Port Security

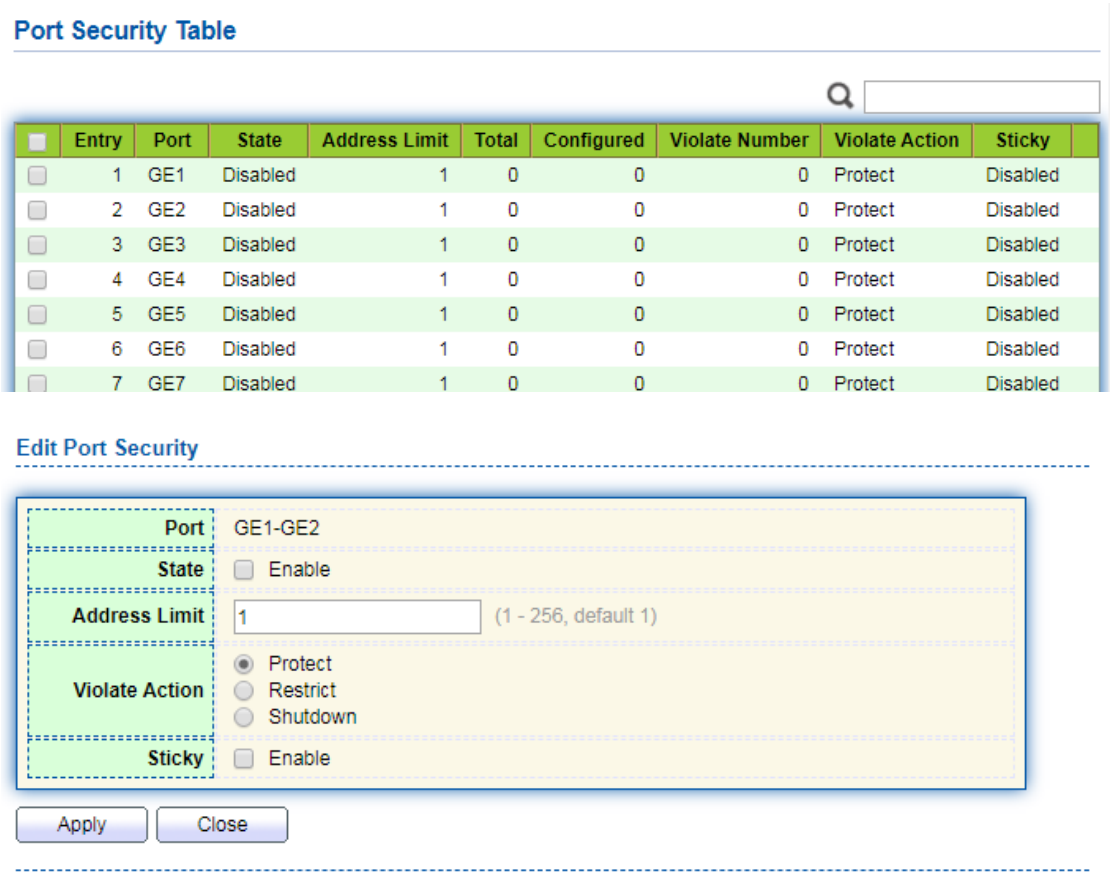
포트 보안 기능은 MAC 주소 테이블을 통해 스위치 포트에 연결된 이더넷 MAC 주소를 기록하고, 이 포트를 통해 하나의 MAC 주소만 통신할 수 있다. 다른 MAC 주소에서 보낸 패킷이 이 포트를 통과할 때 포트 보안 기능이 이를 방지한다. 포트 보안 기능을 사용하면 허가받지 않은 장치가 네트워크에 접속하는 것을 방지하고 보안을 강화할 수 있다. 또한 MAC 주소 범람으로 인해 MAC 주소 테이블이 채워지지 않도록 포트 보안 기능도 사용할 수 있다.

Instructions:

1. 탐색 트리에서 “Port > Port Security”를 클릭하고, 다음과 같이 Port Security 설정을 합니다:



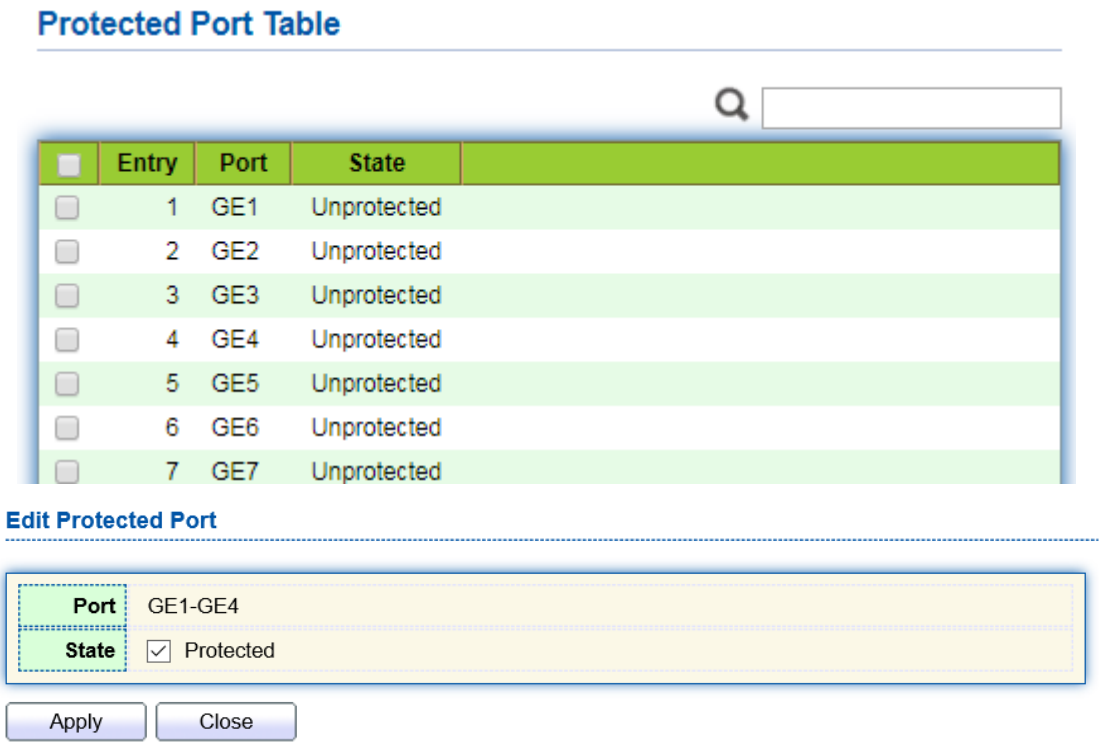
2. 탐색 트리에서 "Port > Port Security"를 클릭하고, 포트를 선택한 다음 "Edit"를 클릭해서 다음과 같이 설정합니다:



5.7 Protected Port

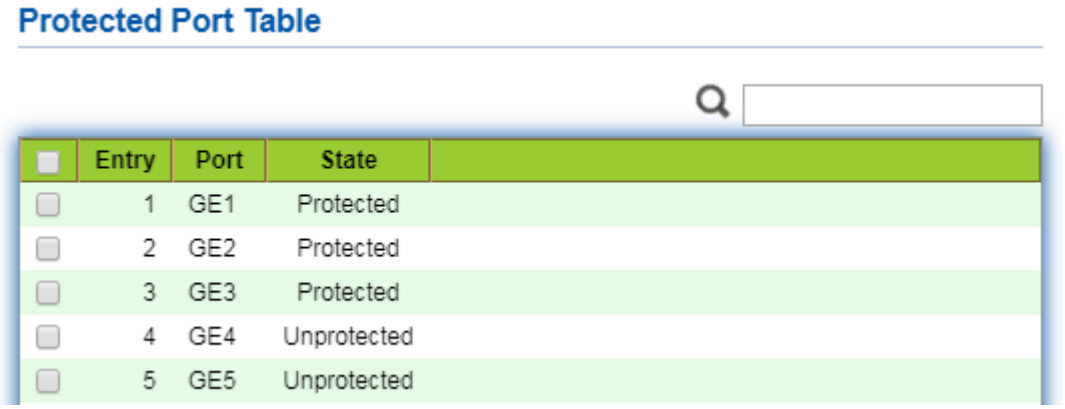
브로드캐스트, 멀티캐스트 등의 메시지는 흐름이 때때로 상호 통신이 필요하지 않더라도 각 포트에 가득 찰 수 있습니다. 이 상황에서 Protected Port 는 두 포트 간에 메시지를 분리할 수 있습니다.

Instructions:
1. 탐색 트리에서 "Port > Protected Port"를 클릭하고, 보호할 포트를 선택한 다음, "Edit"를 클릭하여 다음과 같이 설정합니다:



포트 격리를 위한 방법:

1. 탐색 트리에서 “Port > Protected Port”를 클릭하고, GE1, 2, 3 을 선택한 다음 “Edit”를 클릭합니다. 설정 후 “Apply”를 클릭하여 완료합니다:



2. GE1, 2, 3 은 다른 non-isolated port 처럼 상호간 통신이 불가능합니다.

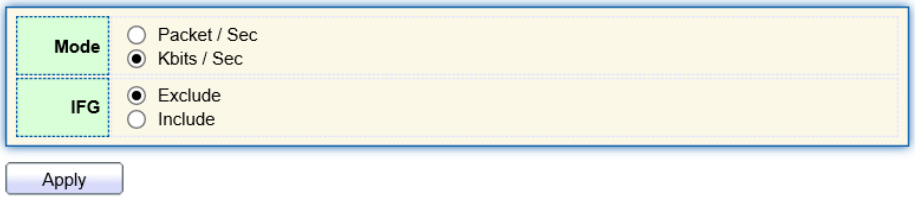
5.8 Storm Control

브로드 캐스트, 알 수 없는 멀티 캐스트 및 유니 캐스트 메시지를 통해 생성된 Storm 은 다음과 같이 방지됩니다. 이러한 메시지는 각각 패킷 속도에 따라 억제됩니다. 모니터링 인터페이스에서 수신한 메시지의 평균 속도는 일정한 검사 간격 동안 구성된 최대 임계 값과 비교됩니다. 평균 속도가 최대 임계 값을

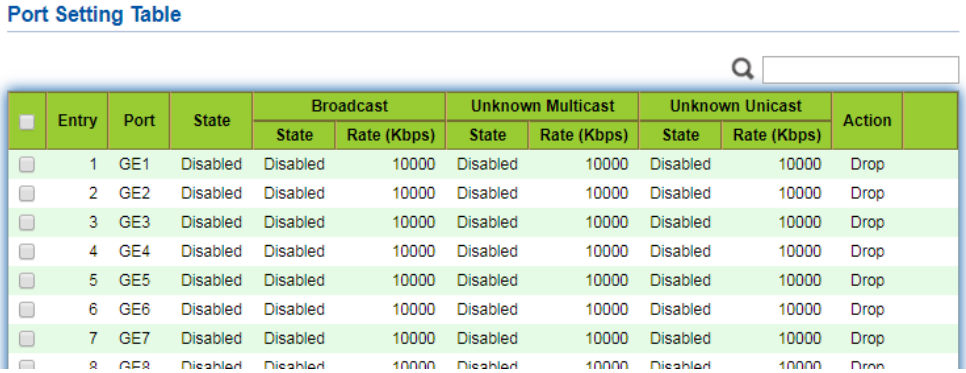
초과하면 구성된 Storm 정책이 이 인터페이스에서 수행됩니다.
L2 이더넷 인터페이스가 브로드 캐스트, 알 수없는 멀티 캐스트 또는 유니 캐스트 메시지를 수신 할 때 대상 MAC 주소에 따라 송신 인터페이스를 인식 할 수 없는 경우 장치는 이를 동일한 VLAN 의 다른 L2 인터페이스로 플러딩합니다. 결과적으로 브로드 캐스트 Storm 이 발생하여 장치 작동 성능이 저하될 수 있습니다. Storm policing 으로 메시지 흐름을 제어하여 브로드 캐스트 Storm 을 피할 수 있습니다.

Instructions:

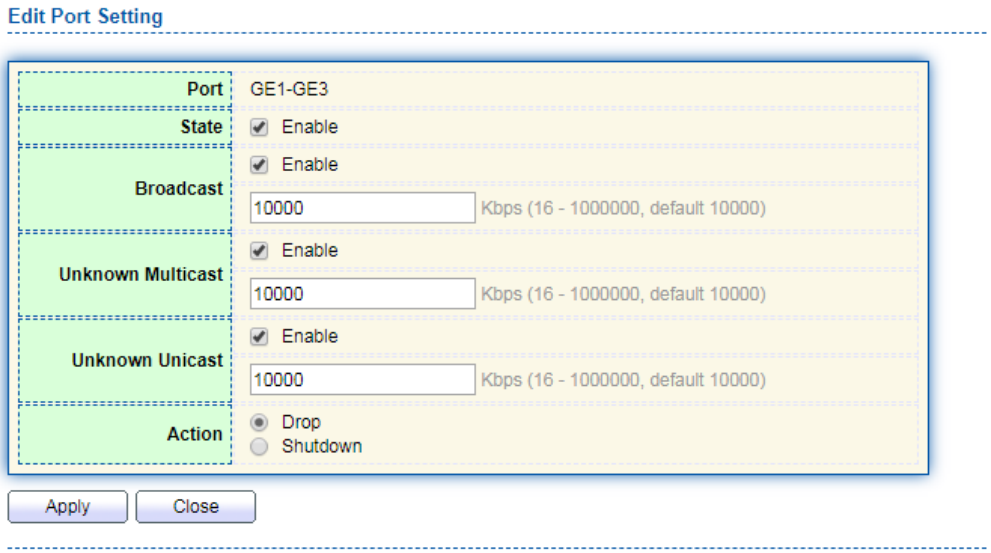
1. 탐색 트리에서 “Port > Storm Control”을 클릭하고, 다음과 같이 설정합니다:



2. 설정할 포트를 선택하고 “Edit”를 클릭하여 다음과 같이 설정합니다.

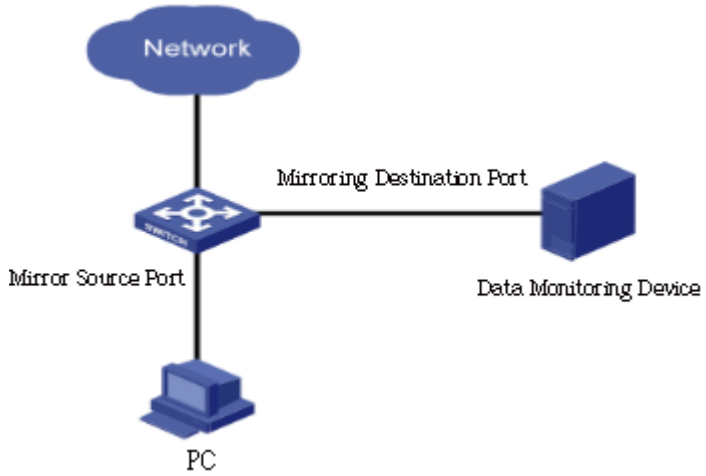


3. storm switch, rate 와 같은 정보를 설정한 다음, “Apply”를 클릭하여 완료합니다:



5.9 Mirroring

포트 미러링은 지정된 스위치 포트의 메시지를 대상 포트로 복사합니다. 복사 된 포트는 소스 포트이고 복사 포트는 대상 포트입니다. 대상 포트는 데이터 검사 장치에 액세스하므로 사용자는 수신된 메시지를 분석하여 네트워크를 모니터링하고 다음과 같이 문제를 해결할 수 있습니다:

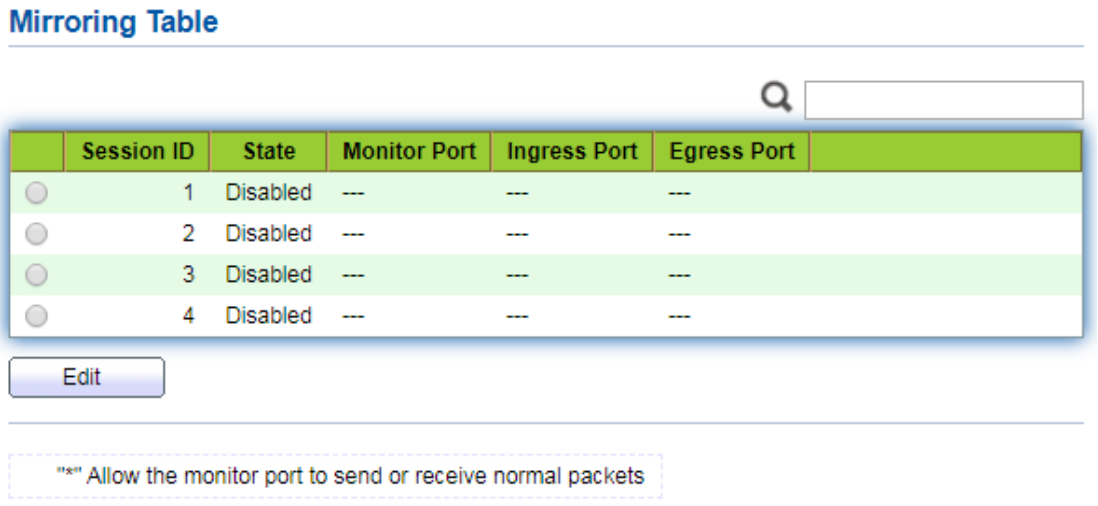


Instance

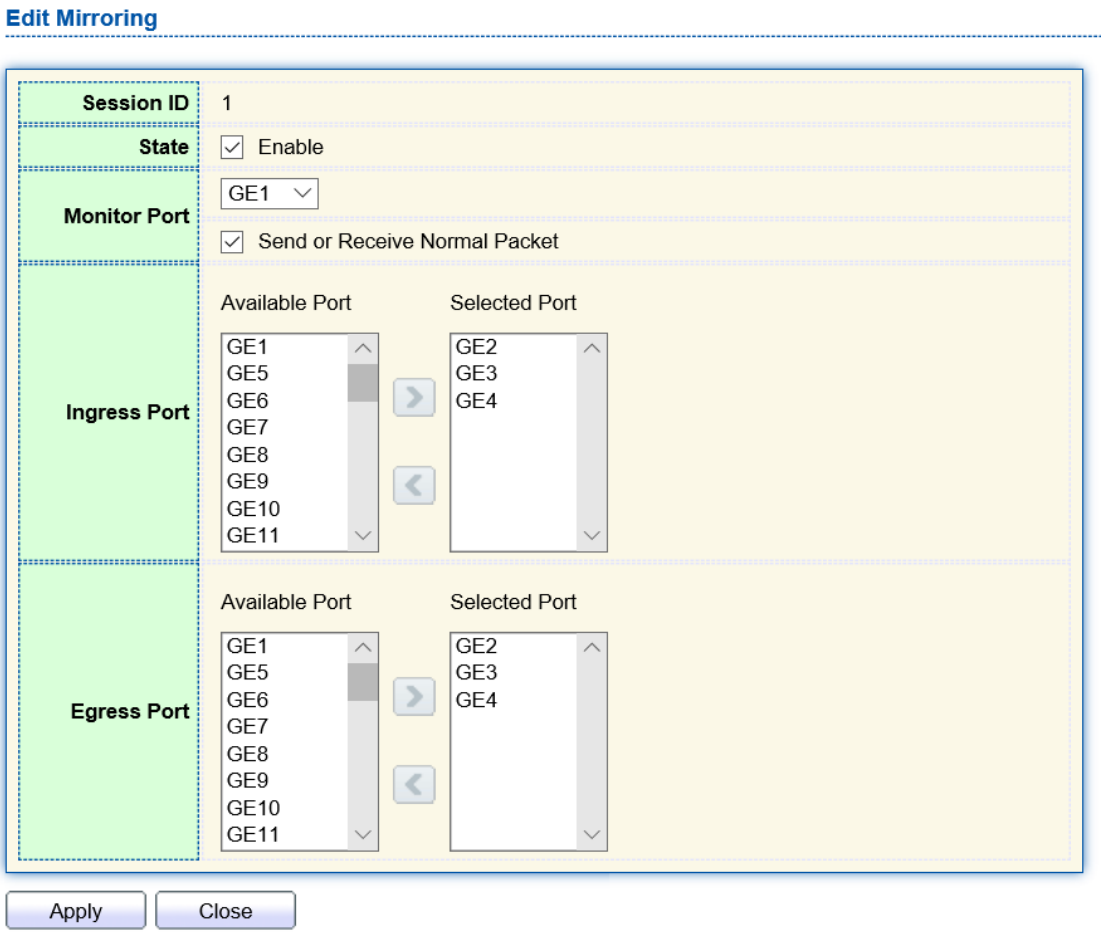
PC1 및 **PC2** 는 각각 인터페이스 **GE1** 및 **GE2** 를 통해 스위치 **A** 에 액세스합니다. 사용자는 **PC2** 에서 **PC1** 로 전송되는 메시지를 모니터링하려고 합니다.

Instructions:

1. 탐색 트리에서 “Port > Mirroring”을 클릭합니다. 다음과 같이 4 개의 미러링 규칙을 구성할 수 있습니다:



2. 세션 하나를 선택하고, “Edit”를 클릭하여 미러링 그룹을 설정합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
Session ID	스위치에는 기본적으로 4 개의 세션 ID 가 있습니다.
State	미러링 그룹을 활성화하거나 비활성화 할 수 있습니다.
Monitor Port	링크 통합 포트 및 소스 포트를 제외한 일반 물리적 포트는 하나만 선택할 수 있습니다..
Ingress Port	수신 된 모든 메시지는 대상 포트로 미러링됩니다.
Egress Port	전송 된 모든 메시지는 대상 포트로 미러링됩니다.

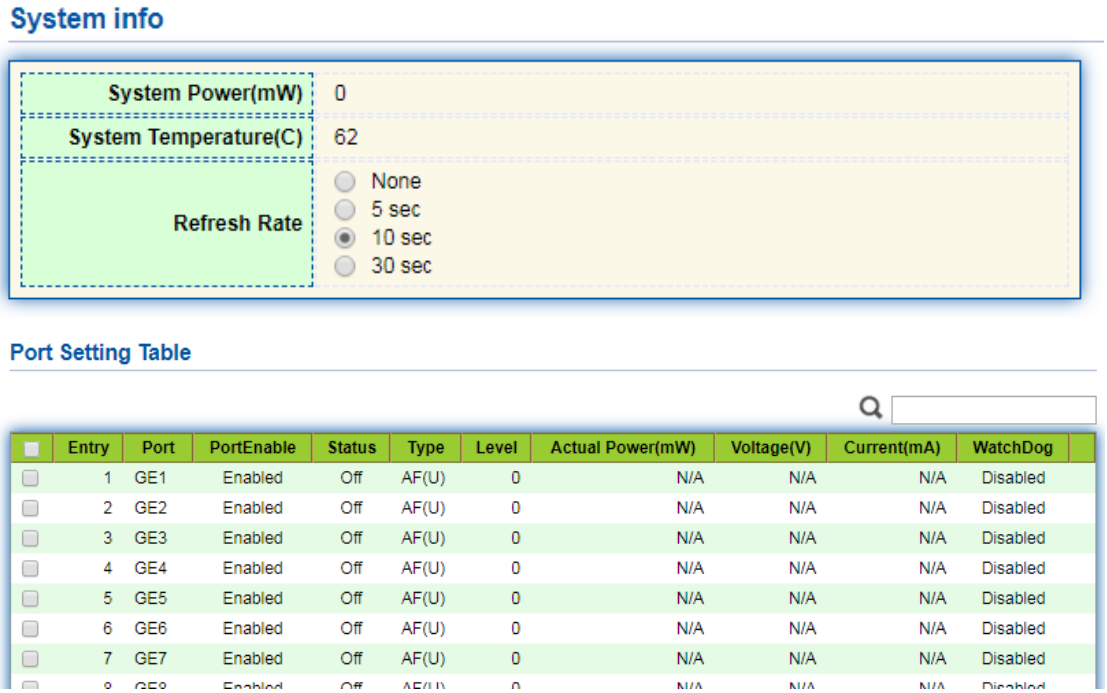
6 POE Setting

PoE(Power over Ethernet)는 IP 를 기반으로한 단말기에 데이터 신호(IP 전화, WAP, IP 카메라)를 전송하며, 기존 Cat-5 네트워크 케이블 연결 상태를 변경하지 않고 직류로 전기를 공급한다. 추가적인 전원 연결 없이 정상적인 네트워크 운영을 보장하여 비용을 최소화한다.

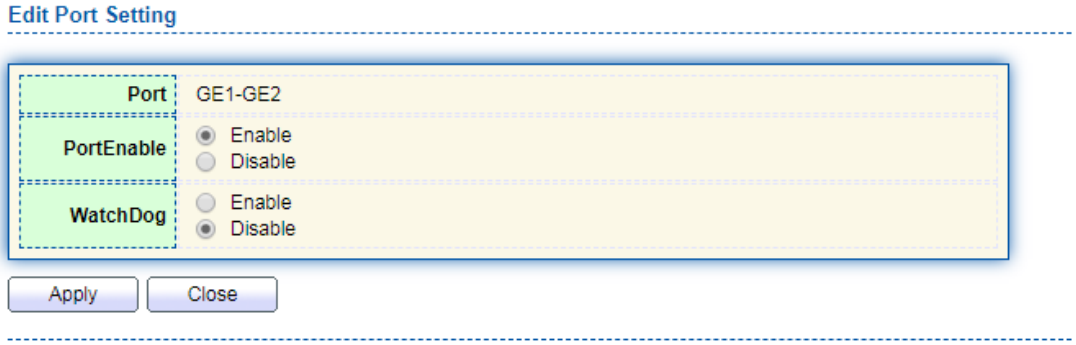
6.1 PoE Port Setting

Instructions:

1. 탐색 트리에서 “POE Setting > POE Port Setting”을 클릭합니다:



2. 설정할 포트를 선택하고, "Edit”를 클릭합니다:



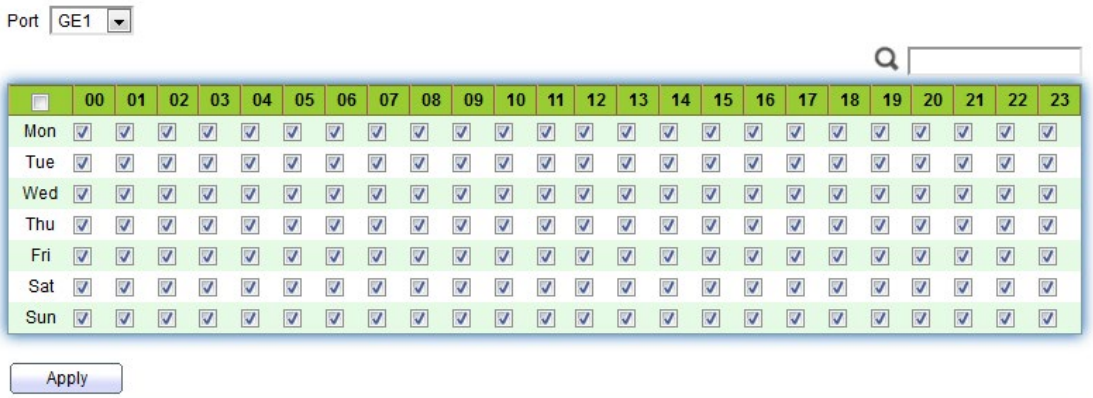
구성 항목은 다음과 같습니다.

구성 항목	설명
PortEnable	Poe port powe 를 활성화/비활성화 합니다.
WatchDog	Poe 포트 감시 기능 활성화/비활성화 합니다. 감시 기능을 활성화한 후 POE 포트의 전원이 계속 공급되지만 트래픽이 없을 때 POE 감시 장치가 트리거됩니다. 2 분간의 감지가 끝나면 전원공급이 정지된 다음 전원을 켭니다. 총 검출 주기는 5 회입니다.

6.2 POE Port Timer Setting

Instructions:

1. 탐색 트리에서 “POE Setting > POE Port Timer Setting”을 클릭하고, 전원 공급 스케줄을 선택합니다:

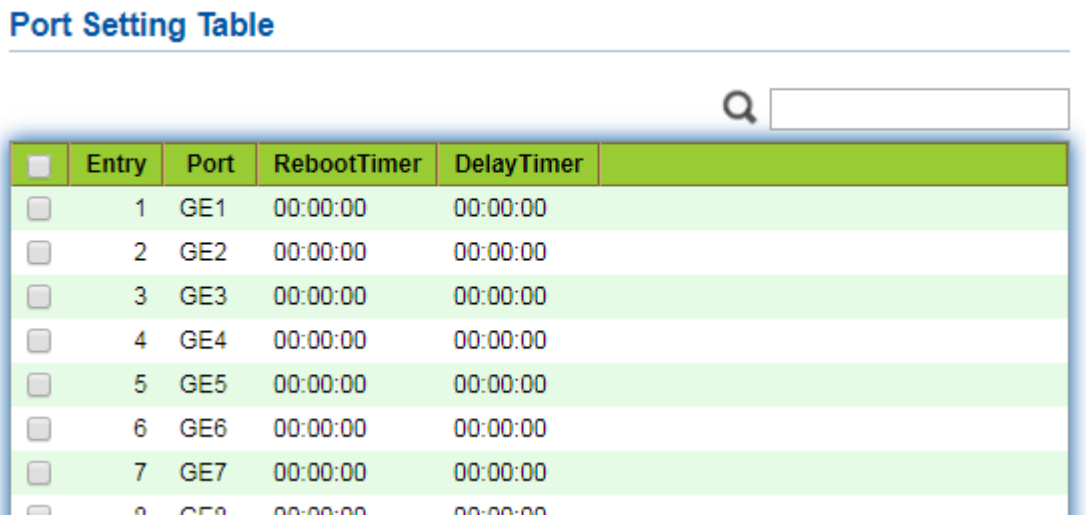


6.3 POE Port Timer Reboot Setting

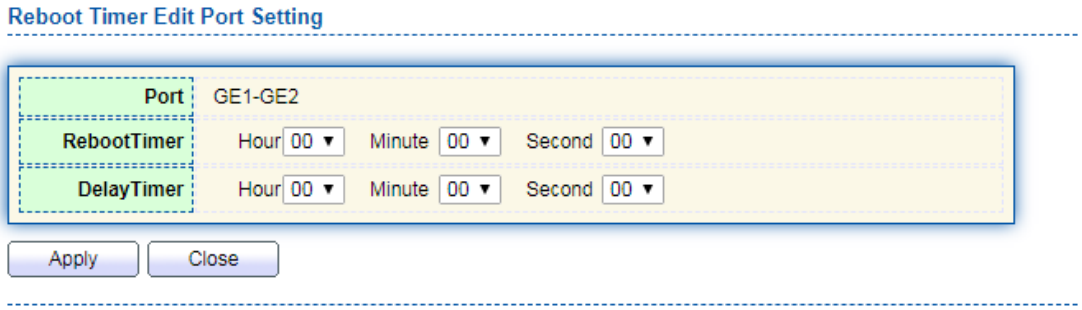
설정을 통해 포트를 기반으로 주기적으로 전원 공급장치를 재가동할 수 있습니다.

Instructions:

1. 탐색 트리에서 “POE Setting > POE Port Timer Reboot Setting”을 선택합니다:



2. 포트를 선택하고, “Edit”를 클릭합니다.



구성 항목은 다음과 같습니다.

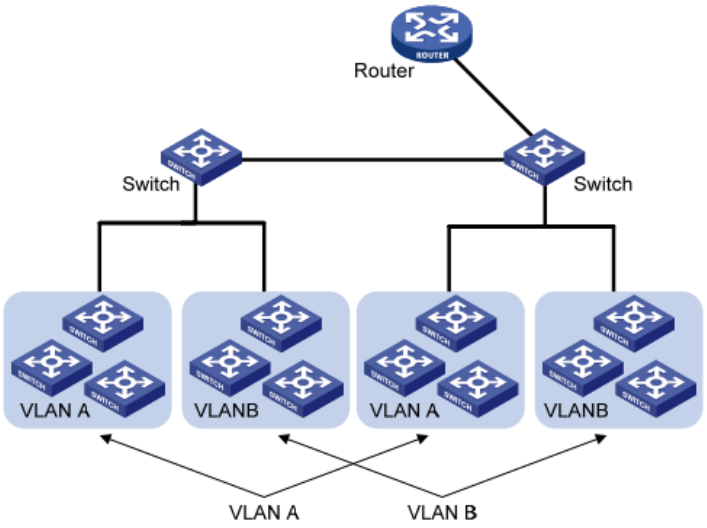
구성 항목	설명
Port	Port 목록
RebootTimer	PoE 포트가 PoE 전원 공급을 끌 때의 시간을 설정합니다. 분 단위의 설정만 가능합니다.
DelayTimer	PoE 전원 공급이 꺼진 후 다시 전원 공급을 시작하는 시간을 설정합니다. 분 단위의 설정만 가능합니다.

Note:

- 이 기능을 사용하기 위해 시스템 시간 동기화를 설정해야 합니다.
- RebootTimer 설정 시, DelayTimer 가 반드시 설정되어야 합니다.
- DelayTimer 가 00:00:00 일 경우, 해당 포트는 더 이상 전원이 공급되지 않음을 의미합니다.

7 VLAN

VLAN 은 물리적 위치에 제한되지 않고 공식화되어 동일한 **VLAN** 의 호스트를 마음대로 배치할 수 있습니다. 아래와 같이 각 **VLAN** 은 브로드 캐스트 도메인으로서 물리적 **LAN** 을 논리적 **LAN** 으로 분할합니다. 호스트는 기존 통신을 통해 메시지를 교환 할 수 있습니다. 다른 **VLAN** 에있는 호스트의 경우 라우터 또는 **L3** 스위치와 같은 장치가 필수입니다.



VLAN 은 다음과 같은 측면에서 기존 이더넷보다 우수합니다:

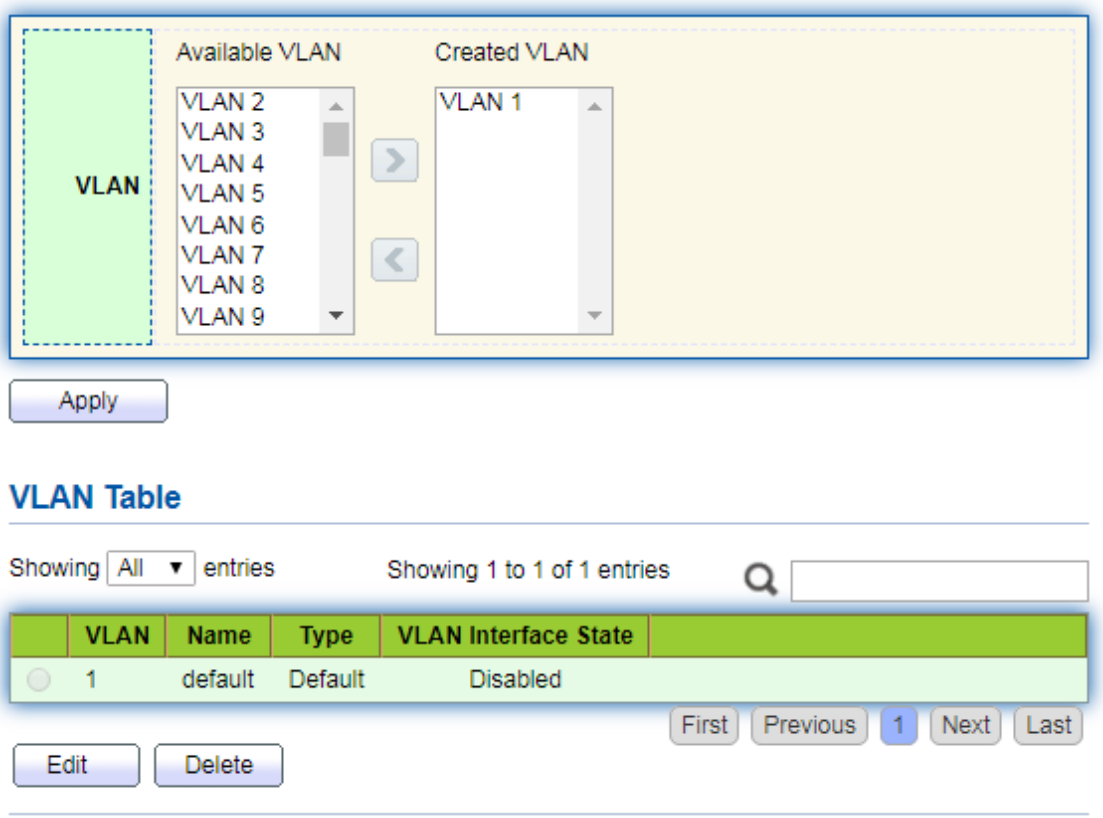
- Broadcast domain coverage: **LAN** 의 브로드 캐스트 메시지는 대역폭을 절약하고 네트워크 관련 문제를보다 효율적으로 처리하기 위해 **VLAN** 에서 제한됩니다.
- LAN security: 데이터 링크 계층에서 메시지가 브로드 캐스트 도메인으로 분리되므로 **VLAN** 호스트가 서로 통신하지 못합니다. 레이어 **3** 포워딩을 위해 라우터 또는 레이어 **3** 스위치가 필요합니다.
- 가상 작업 팀을 만드는 유연성: **VLAN** 은 물리적 네트워크의 제어를 넘어 가상 작업 팀을 만들 수 있습니다. 사용자는 물리적 위치가 범위 내에서 이동하는 경우 구성을 변경하지 않고 네트워크에 액세스 할 수 있습니다.
  이 관리 스위치는 **802.1Q,** 프로토콜**, MAC** 및 포트를 기반으로하는 **VLAN** 유형과 호환됩니다. 기본 구성의 경우 **802.1Q VLAN** 모드를 채택해야합니다.
  포트 **VLAN** 은 스위치의 인터페이스 번호에 따라 구분됩니다. 네트워크 관리자는 각 스위치 인터페이스에 서로 다른 **PVID,** 즉 포트 기본 **VLAN** 을 제공합니다. **VLAN** 태그가없는 데이터 프레임이 **PVID** 를 사용하여 스위치 인터페이스로 유입되면 동일한 **PVID** 로 표시되거나 인터페이스에 **PVID** 가 있어도 추가 태그가 제거됩니다.
- **VLAN** 프레임에 대한 솔루션은 인터페이스 유형에 따라 달라 지므로 구성원 정의가 쉬워 지지만 구성원 이동성의 경우 **VLAN** 을 재구성합니다.

7.1 VLAN

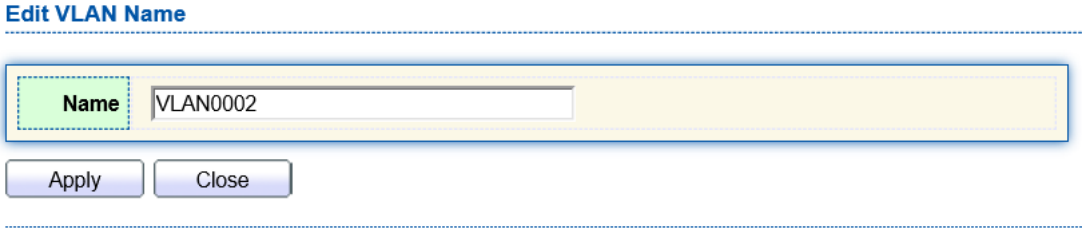
7.1.1 Create VALN

새 VLAN 을 만드는 방법:

1. 탐색 트리에서 “VLAN > VLAN > Create VLAN” 를 클릭하여 유효한 **VLAN** 상자에서 이름을 선택하고 오른쪽의 **VLAN** 생성 상자로 이동합니다 **(**최대 **256** 개의 **VLAN** 생성 가능**).** 다음과 같이 “Apply” 하고 완료합니다:



2. 생성된 **VLAN** 이 **VLAN** 테이블에 표시됩니다. 사용자는 다음과 같이 **VLAN** 을 수정할 수 있습니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN ID	**1 ~ 4,094** 범위의 **ID** 를 선택해야합니다. 예를 들어 **1-3,5,7** 및 **9** 입니다. **LAN 1** 이 기본값이며 다른 새 **VLAN** 에서 반복되지 않습니다.
Name	필요에 따라 **VLAN** 설명을 수정합니다(선택 사항)

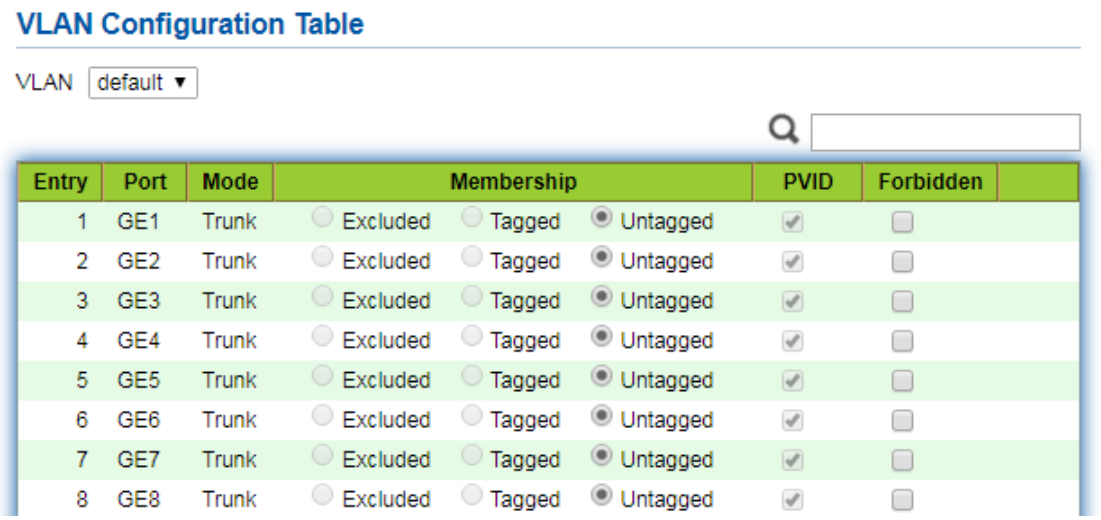
7.1.2 VLAN Configuration

두 가지 방법이 있습니다. 하나는 단일 **VLAN** 아래에 여러 포트를 추가하는 것입니다.

다른 하나는 여러 **VLAN** 에 포트를 추가하는 것입니다. 그들은 다른 목적에 따라 구성됩니다.

특정 **VLAN** 에 포트를 추가하는 첫번째 방법

1. 탐색 트리에서 "VLAN > VLAN > VLAN Configuration" 을 클릭하고, 좌측 상단의 VLAN ID 를 선택한 뒤, 다음과 같이 포트 정보를 클릭하십시오:



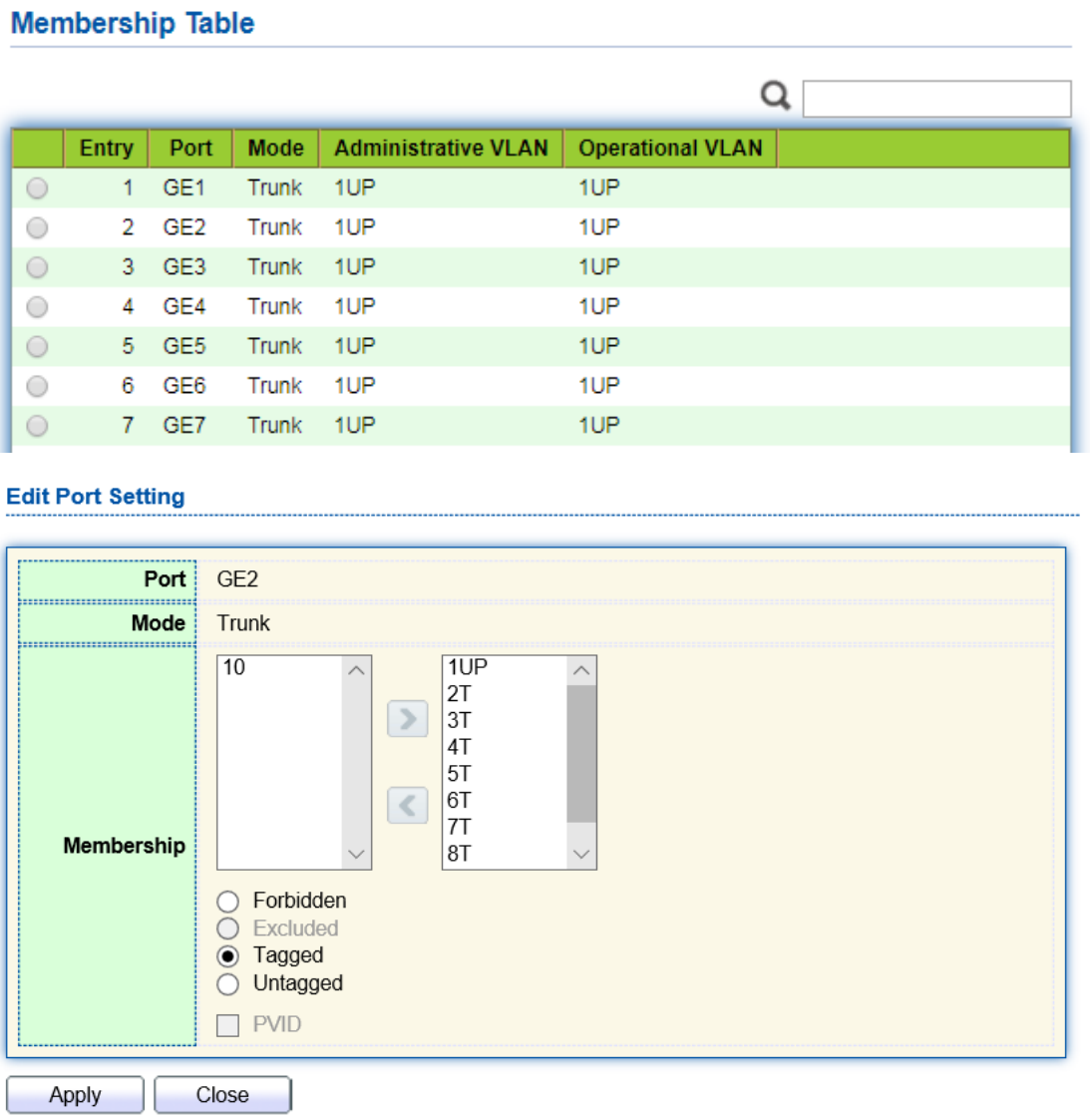
구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	**VLAN ID**
Port	포트
Mode	포트의 VLAN 모드
Membership	**VLAN** 포트의 구성원 역할: Excluded: 포트가 이 **VLAN** 에 속하지 않습니다 Tagged: 포트는 이 **VLAN** 의 태그가 지정된 구성원입니다 Untagged: 포트는 이 **VLAN** 의 태그가 지정되지 않은 구성원입니다
PVID	이 **VLAN** 이 포트 **PVID** 인지 여부
Forbidden	**VLAN** 메시지가 이 포트에서 전달되는 것이 금지되어 있는지 여부

7.1.3 Membership

특정 **VLAN** 에 포트를 추가하는 두번째 방법

1. 탐색 트리에서 "VLAN > VLAN > Membership" 을 클릭하고, 포트를 선택한 다음 수정하여 속성을 설정합니다:



구성 항목은 다음과 같습니다.

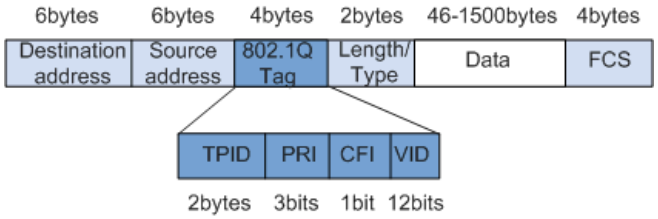
구성 항목	설명
Port	포트 번호
Mode	현재 **VLAN** 모드를 수정합니다: Hybrid: 이 모드의 포트는 **VLAN** 의 **Tagged & Untagged** 멤버 역할을 할 수 있습니다. Access: 이 모드의 포트는 **VLAN** 의 유일한 구성원 역할을 합니다. Trunk: 이 모드의 포트는 **PVID** 의 태그가 지정되지 않은 구성원과 **VLAN** 의 태그가 지정된 구성원으로만 사용됩니다
Membership	**VLAN ID** 및 **VLAN** 의 속성입니다: Forbidden: **VLAN** 메시지를 전달하지 않습니다. Excluded: **VLAN** 외부의 포트입니다.

	Tagged: **VLAN** 의 태그된 구성원입니다. Untagged: 태그가 지정되지 않은 **VLAN** 구성원입니다. PVID: **VLAN** 이 **PVLAN** 포트인지 여부를 표시합니다.

7.1.4 Port Setting

트렁크 구성. 다른 스위치와 연결되는 트렁크 인터페이스는 주로 트렁크 링크를 연결하여 **VLAN** 프레임이 통과 할 수 있도록합니다. **IEEE 802.1q** 는 트렁크 링크의 캡슐화 프로토콜이며 **Virtual Bridged Local Area Networks** 의 공식 표준을 고려합니다. 소스 **MAC** 주소 필드와 프로토콜 필드 사이에 **4** 비트 **802.1q** 태그를 추가하여 이더넷의 프레임 형식을 변경합니다.

802.1q frame format

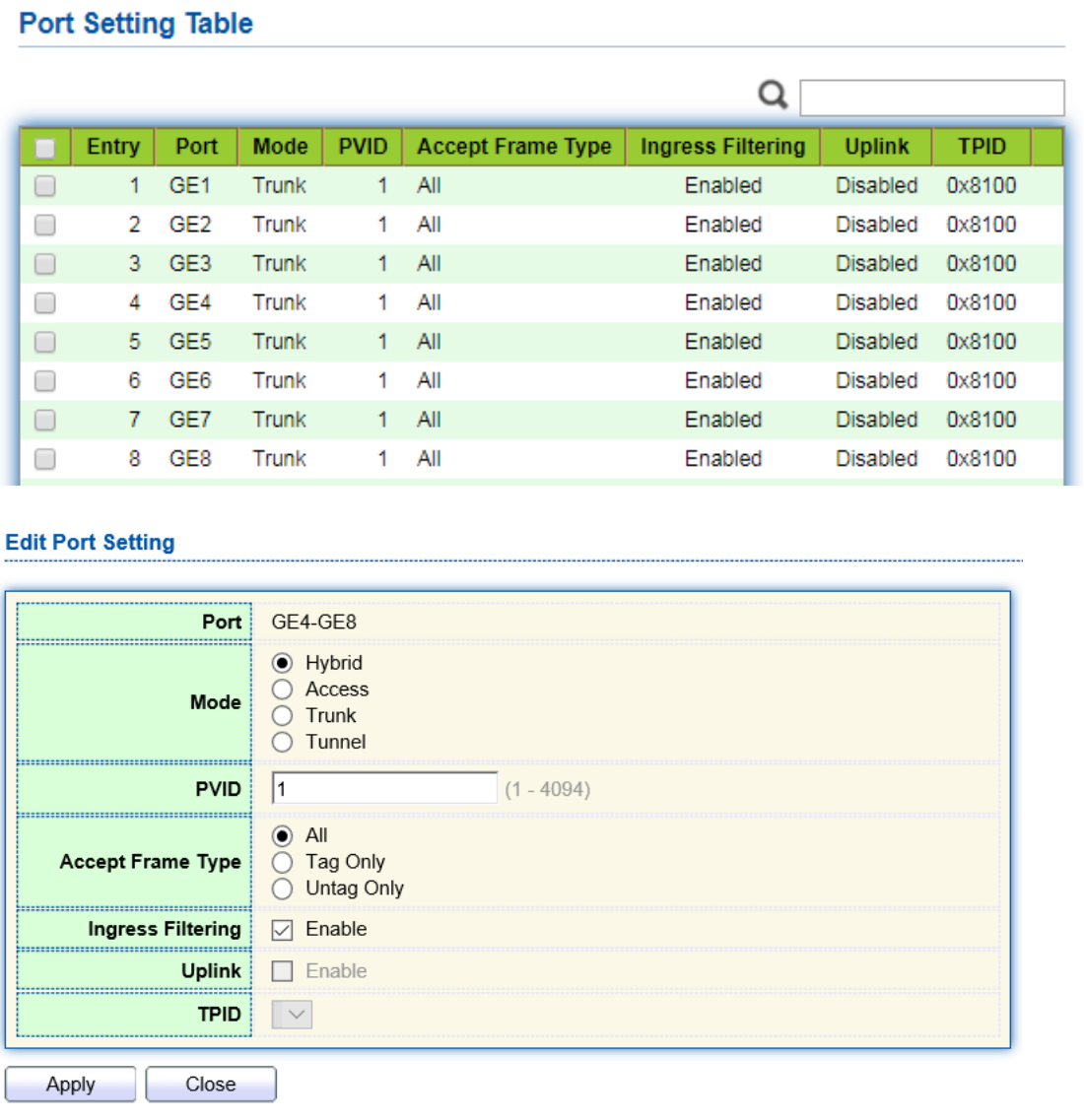


802.1q 태그 필드의 의미

필드	길이	이름	분석
TPID	2 bytes	**Tag Protocol Identifier** 로 프레임 유형을 설명합니다	값이 **0x8100** 일 때 **802.1q** 태그 프레임을 말하며, 관련 장비가 수신하지 못할 경우 폐기됩니다.
PRI	3 bits	프레임 우선순위	**0** 에서 **7** 까지의 범위이며 높은 우선 순위는 더 큰 숫자로 표시됩니다. 스위치 혼잡시 우선 순위가 높은 데이터 프레임이 우선적으로 전송됩니다.
CFI	1 bit	**MAC** 주소가 클래식인지 여부를 표시하는 **Canonical Format Indicator**	**MAC** 주소는 **CFI** 가 **0** 이면 클래식이고 **CFI** 가 **1** 이면 비 클래식입니다. 이더넷과 토큰 링 간의 호환성을 촉진합니다. 이더넷에서 **CFI** 는 **0** 입니다.
VID	12 bits	**VLAN ID** 는 프레임이 속한 **VLAN** 을 나타냅니다.	**0** 과 **4,095** 가 프로토콜 보존 값이므로 **0** 에서 **4,095** 까지의 범위이며 **1** 에서 **4,094** 까지 유효합니다.

802.1q 프로토콜을 지원하는 각 스위치에서 보낸 패킷에는 스위치가 속한 **VLAN** 을 나타내는 **VLAN ID** 가 포함되어 있습니다. 따라서 이더넷 프레임은 **VLAN** 스위칭 네트워크에서 다음과 같이 두 가지 유형으로 나뉩니다:
- Tagged frame: **4** 비트 **802.1q** 태그를 추가하는 프레임을 의미합니다.
- Untagged frame: **4** 비트 **802.1q** 태그가없는 원본 프레임을 나타냅니다..
다른 스위치와 연결되는 트렁크 인터페이스는 주로 트렁크 링크를 연결하여 **VLAN** 프레임이 통과 할 수 있도록합니다.

트렁크 인터페이스 구성 방법:
1. 탐색 트리에서 “VLAN > VLAN > Port Setting”을 클릭하고 포트를 선택한 다음 수정합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
Port	포트 번호
Mode	포트 구성에서 현재 **VLAN** 모드를 수정합니다: Hybrid: 이 모드의 포트는 **VLAN** 의 **Tagged** 및 **Untagged** 포트의 구성원 역할을 합니다 Access: 이 모드의 포트는 **VLAN** 의 유일한 구성원 역할을 합니다 Trunk: 이 모드의 포트는 **PVID** 의 유일한 **Untagged** 구성원 및 **VLAN** 의 **Tagged** 구성원 역할을 합니다.
PVID	Port PVLAN
Accept Frame Type	포트에서 수신한 메시지 유형 All: 모든 메시지 Tag Only: 태그가 지정된 메시지만 수신됩니다. Untag Only: 태그가 지정되지 않은 메시지만 수신됩니다.
Ingress Filtering	포트에서 제외된 **VLAN** 메시지를 필터링하기로 결정한 스위치
Uplink	업 링크 모드 여부
TPID	**VLAN** 태그의 식별 번호

7.2 Voice VLAN

기존에는 음성 데이터를 구분하기 위해 **ACL (Access Control List)**을 적용하고 전송 품질을 보장하기 위해 **QoS (Quality of Service)**를 사용하여 우선 순위를 높였습니다. 현재는 사용자 구성을 단순화하고 음성 흐름 관리를 용이하게하기 위해 Voice **VLAN** 이 등장하였습니다. 활성화된 인터페이스는 인터페이스 데이터 흐름에 액세스하는 소스 **MAC** 주소 필드에 따라 음성 데이터 흐름인지 여부를 판단합니다. 소스 **MAC** 주소의 메시지는 시스템에서 구성한 음성 장치의 **OUI (Organizationally Unique Identifier)**를 확인하는 음성 데이터 흐름입니다. 음성 데이터 흐름을 수신하는 인터페이스는 자동으로 Voce **VLAN** 으로 전송되므로 사용자 구성 및 음성 데이터 관리가 단순화됩니다.

Voice VLAN 의 OUI

OUI 는 **MAC** 주소 필드를 나타냅니다. 주소는 **48** 비트 **MAC** 주소와 해당 마스크 비트를 기반으로 계산할 수 있습니다. 수신 **MAC** 주소와 일치하는 **OUI** 의 비트 수는 마스크의 모든 **"1"**비트 길이에 의해 결정됩니다. 예를 들어 **MAC** 주소가 **1-1-1** 이고 마스크가 **FFFF-FF00 - 0000** 인 경우 **MAC** 주소 및 해당 마스크, 즉 **OUI** 의 실행 및 계산 결과는 **0001 - 0000 - 0000** 이됩니다.
수신 **MAC** 주소의 처음 **24** 비트가 **OUI** 의 것과 일치하는 한 활성화 된 Voice **VLAN** 인터페이스는 데이터 흐름과 수신 장치를 각각 음성 데이터 흐름 및 음성 장치로 식별합니다.

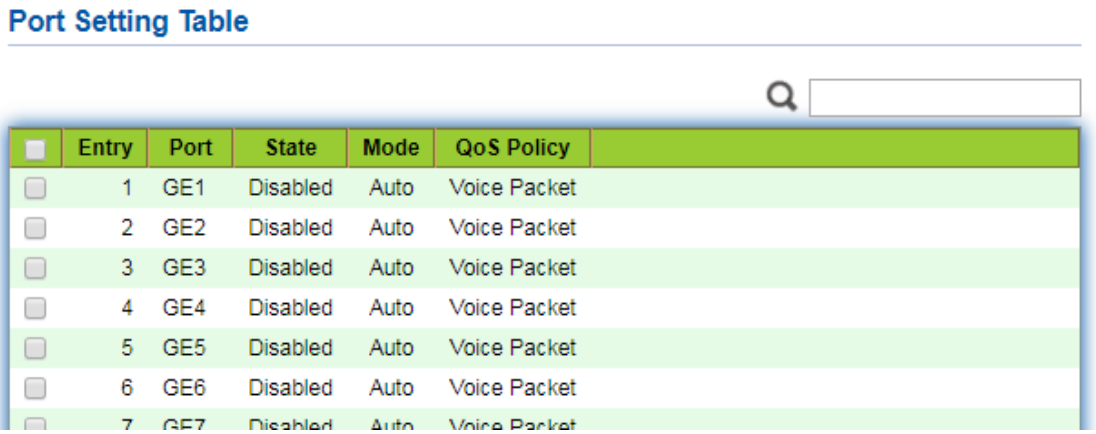
Voice **VLAN** 은 사용자 음성 데이터 흐름을 위해 나뉩니다. Voice **VLAN** 은 음성 장치와 연결된 인터페이스를 연결하여 중앙 집중식으로 음성 데이터를 내부로 전송하기 위해 생성됩니다.
음성 데이터와 비 음성 데이터는 종종 동일한 네트워크에 존재합니다. 음성 데이터는 가능한 지연 및 패킷 손실을 줄이기 위해 전송 중에 다른 비즈니스 데이터보다 더 높은 우선 순위가 필요합니다.

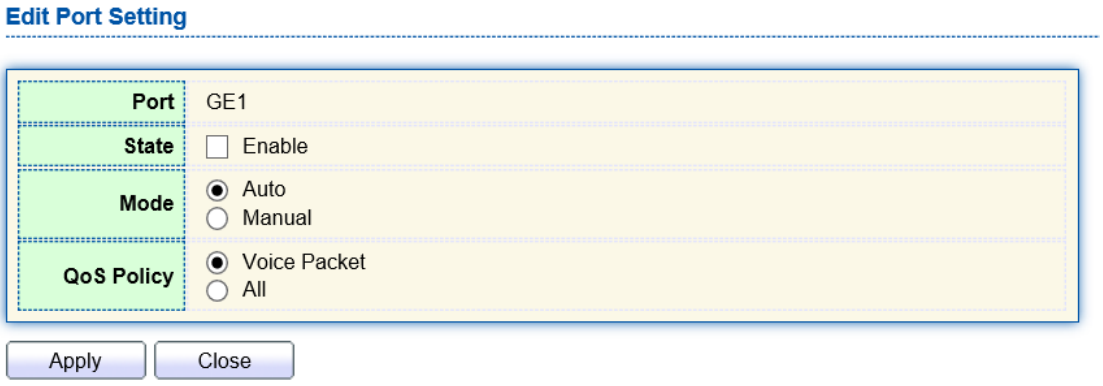
1. 탐색 트리에서 "VLAN > Voice VLAN > Property"을 클릭합니다.



구성 항목은 다음과 같습니다.

구성	설명
State	Voice **VLAN** 확인 및 활성화
VLAN	추가된 **VLAN ID** 를 **1 ~ 4,094** 범위로 지정합니다 **(**예 **: 1-3, 5, 7** 및 **9 (**기본적으로 **VLAN 1** 포함**).** 다른 **VLAN** 은 링크가 필요한 포트에 태그없는 방식으로 추가해야합니다.
CoS Remark	Voice **VLAN** 메시지 우선 순위를 재정의할지 여부
Aging Time	Table aging time



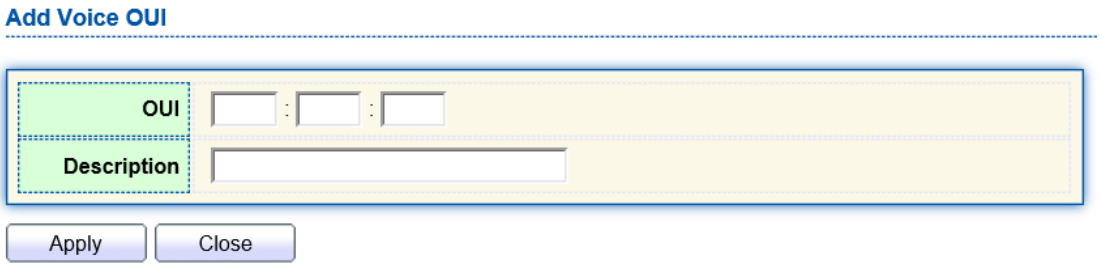


구성 항목은 다음과 같습니다.

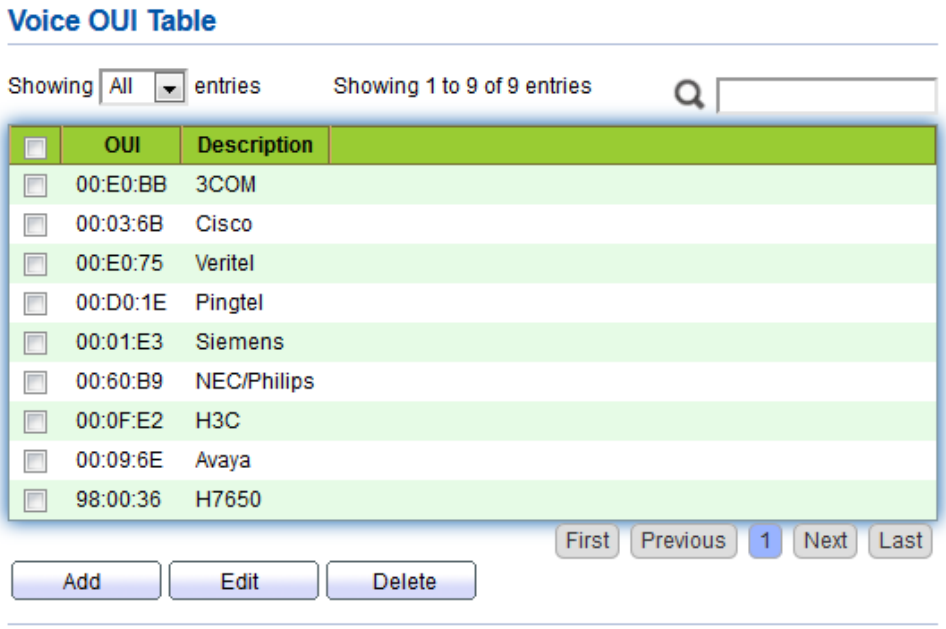
구성 항목	설명
Port	활성화 된 Voice **VLAN** 포트
State	Voice VLAN 활성화 상태
Mode	Voice **VLAN** 포트는 자동 모드와 수동 모드에서 작동 할 수 있습니다.
QoS Policy	**QoS** 의 영향을 받을 메시지 선택

2. 탐색 트리에서 “VLAN > Voice VLAN > Voice OUI” 을 클릭하여 음성 **VLAN** 의 **OUI** 주소 세그먼트를 다음과 같이 구성합니다:

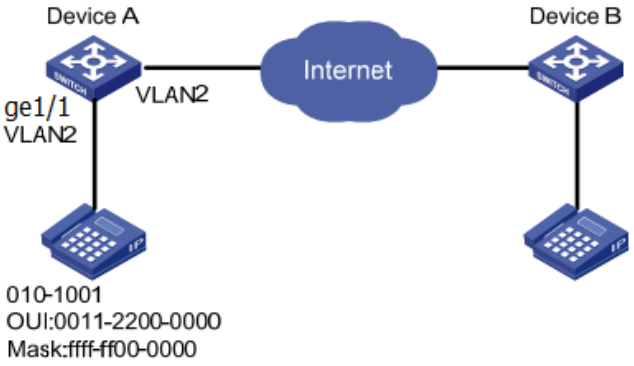




3. 해당 구성 항목을 입력합니다.
4. “Apply”하고 다음과 같이 마칩니다.

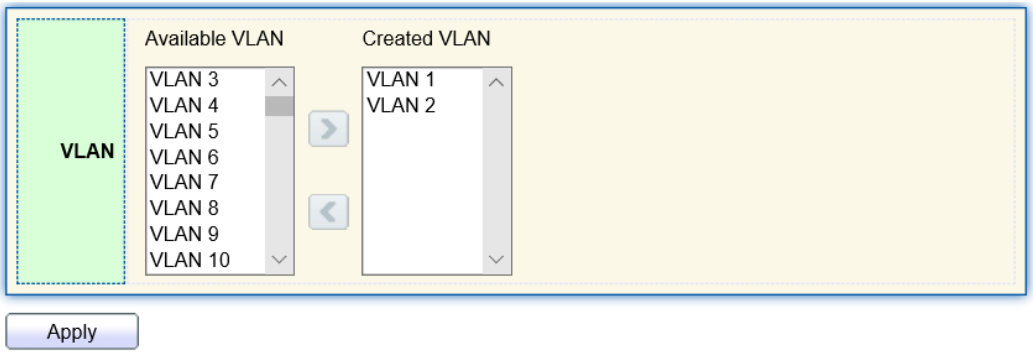


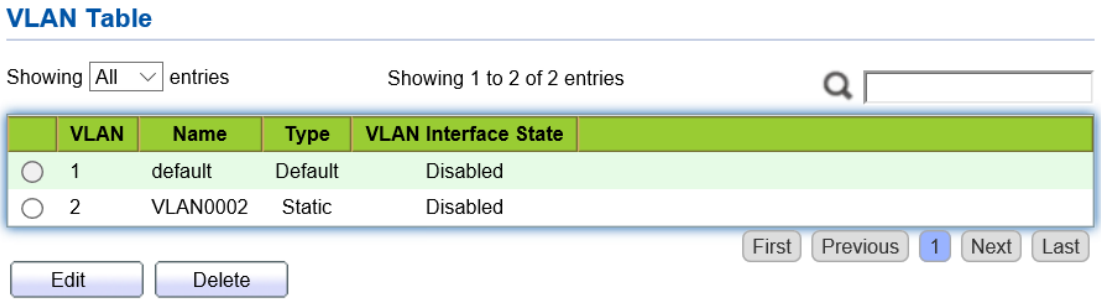
예를 들어, **IP** 텔레포니에 액세스하는 포트가 Voice **VLAN** 을 들어오고 나가고 그 안에서 음성 흐름을 전송할 수 있도록 수동 모드에서 Voice **VLAN** 을 구성합니다. **VLAN2** 를 생성하여 Voice **VLAN** 을 안전하게 운영하면 음성 데이터만 통과할 수 있습니다. **IP** 텔레포니는 태그가 지정되지 않은 음성 흐름을 수신 트렁크 포트인 **GE1** 로 전송합니다. 사용자는 **OUI (0011-2231-05e1)**를 사용자 지정하고 자동 모드에서 Voice **VLAN** 네트워킹 다이어그램을 구성해야합니다.



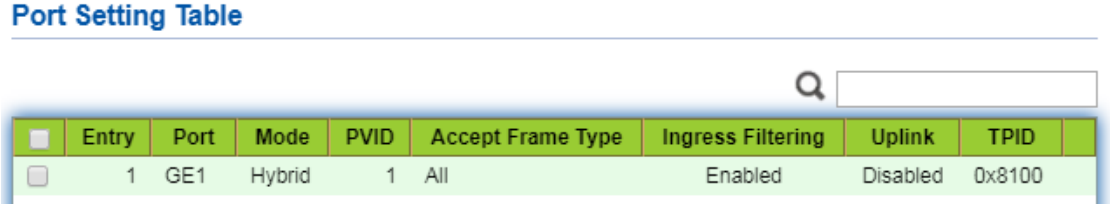
Instructions:

1. 직원이 속한 VLAN 을 인식하는 VLAN 을 만듭니다. 탐색 트리에서 "VLAN > VLAN > Create VLAN" 을 클릭하여 오른쪽의 VLAN 목록에 VLAN2 를 추가합니다. "Apply" 하여 완료합니다:

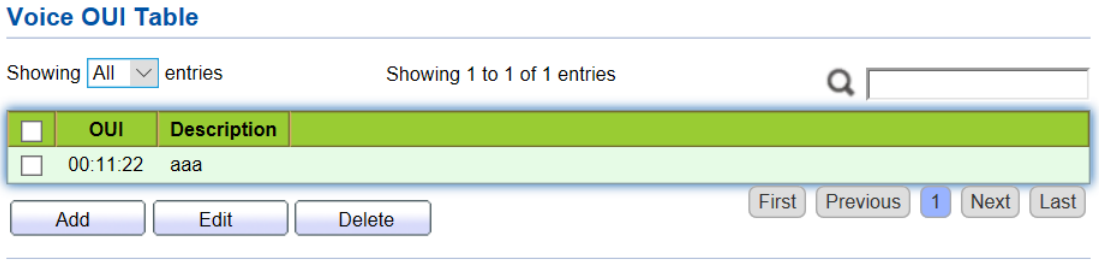




2. 하이브리드 모드에서 스위치 **A** 의 이더넷 인터페이스 **GE1** 을 구성합니다. 탐색 트리에서 "VLAN > VLAN > Port Setting" 을 클릭하고 하이브리드 모드에서 **GE1** 을 "Edit"합니다:

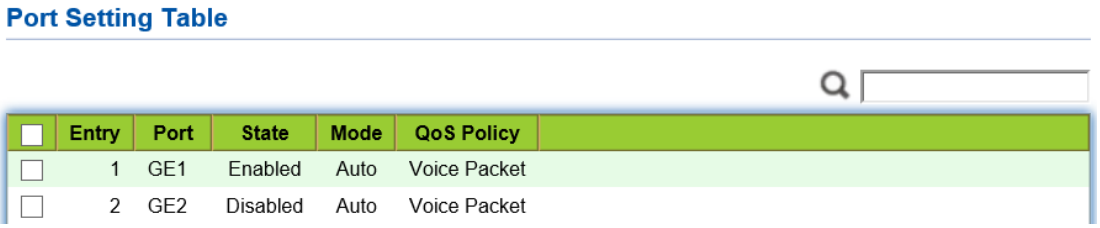


2. 탐색 트리에서 “VLAN > Voice VLAN > Voice OUI” 을 클릭하여 **OUI MAC** 주소 범위를 구성 및 추가하고 음성 장치 **MAC** 주소의 처음 **24** 비트를 입력합니다 : **00:11:22.** 다음과 같이 "Apply"하고 완료합니다:



3. 포트 **GE1** 의 Voice VLAN 을 활성화합니다. 탐색 트리에서 “VLAN > Voice VLAN > Property” 을 클릭하여 글로벌 구성을 활성화하고 **VLAN2** 를 선택합니다. 구성 목록에서 포트 **GE1** 을 선택하고 자동 모드를 활성화합니다:





Note:

- 자동 모드를 활성화하면 **VLAN2** 에 포트가 없더라도 포트가 Voice **VLAN** 메시지를 전달합니다.

7.3 Protocol VLAN

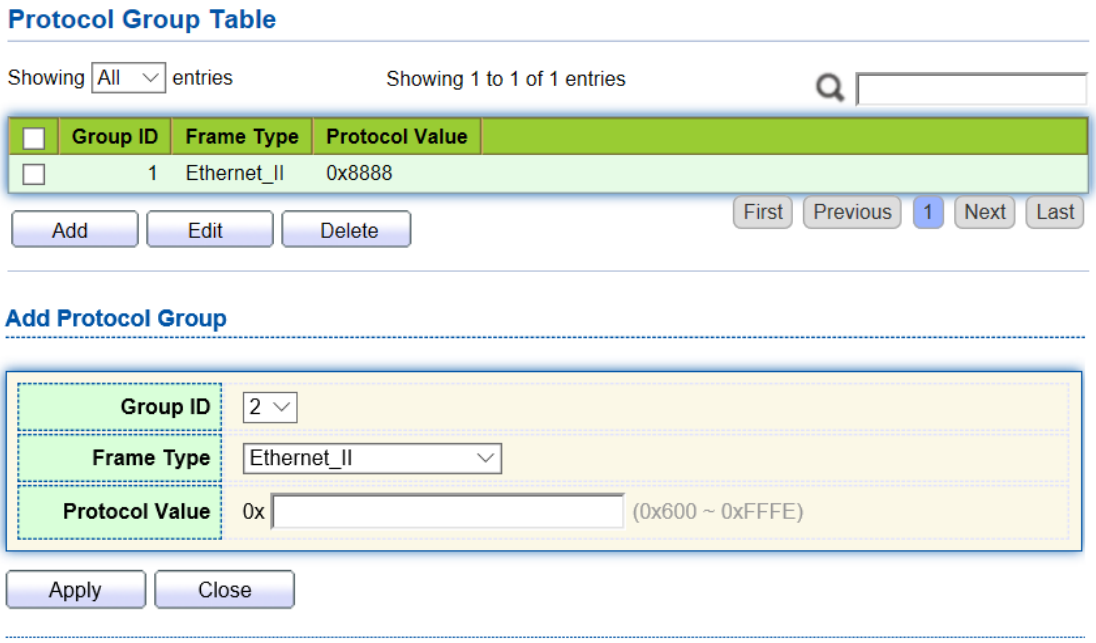
프로토콜 기반 **VLAN** 은 인터페이스에서 수신한 메시지의 프로토콜(family) 유형 및 캡슐화 형식에 따라 서로 다른 **VLAN ID** 를 배포합니다.

관리자는 이더넷 프레임의 프로토콜 도메인과 태그가 지정되지 않은 프레임이 수신되면 추가될 **VLAN ID** 간의 매핑 체계를 준비해야합니다.

- 장점 : 이러한 분할 방법은 네트워크 서비스와 **VLAN** 을 바인딩하여 관리 및 유지 관리를 향상시킵니다.
- 단점 : 매핑 관계 체계의 초기 구성이 필요합니다. 프로토콜의 주소 형식을 분석하고 변환해야하므로 많은 리소스가 소비되므로 속도가 느려집니다.

Instructions:

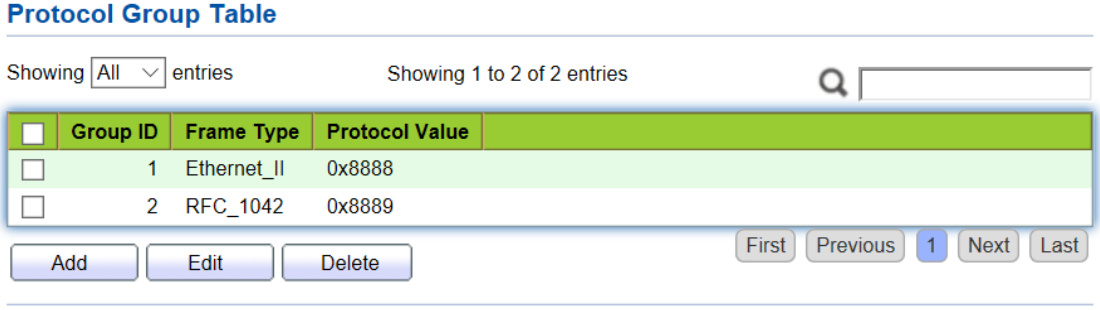
1. 탐색 트리에서 “VLAN > Protocol VLAN > Protocol Group”을 클릭합니다:



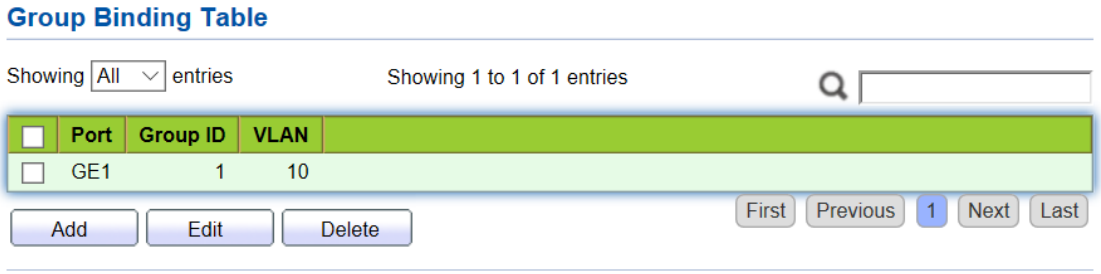
구성 항목은 다음과 같습니다.

구성 항목	설명
Group ID	Protocol VLAN Group
Frame Type	프레임 타입: Ether2, LLC, RFC 1042
Protocol Value	0x6000 과 0xFFFE 범위

2. 해당 구성 항목을 입력합니다.
3. “Apply”하고 마칩니다.



4. 탐색 트리에서 “VLAN > Protocol VLAN > Group Binding”을 클릭하여 프로토콜 번호, 포트 번호 및 VLAN ID를 바인딩하고 다음과 같이 설정을 적용합니다:

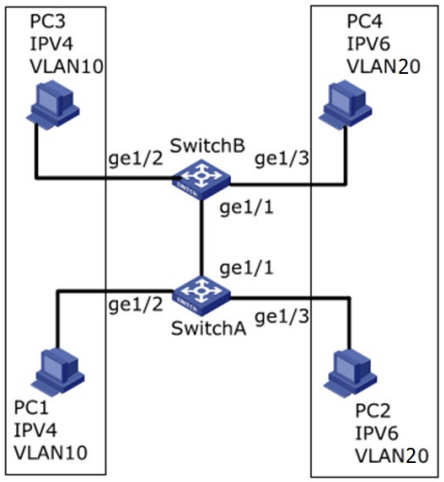


Description:

일치하는 프로토콜 **IPv4** 및 **IPv6** 와 **ARP** 프로토콜을 구성합니다..

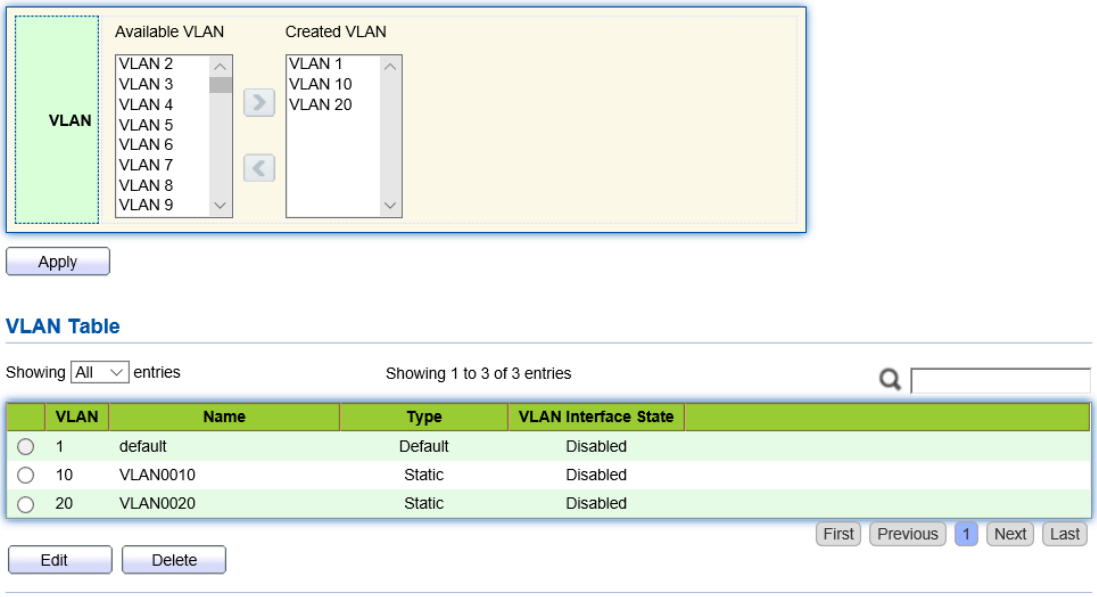
예를 들어 **PC1** 과 **3** 은 **VLAN10** 과의 **IPv4** 통신 프로토콜 바인딩을 통해 상호 액세스 할 수 있습니다. **PC2** 및 **4** 는 **VLAN20** 과의 **IPv6** 통신 프로토콜 바인딩을 통해 상호 액세스 할 수 있습니다.

프로토콜 **VLAN** 분할의 네트워킹 다이어그램

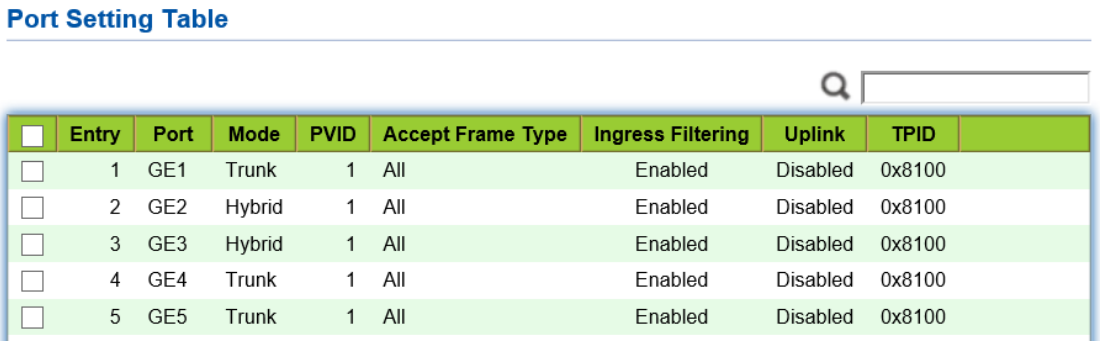


Instructions:

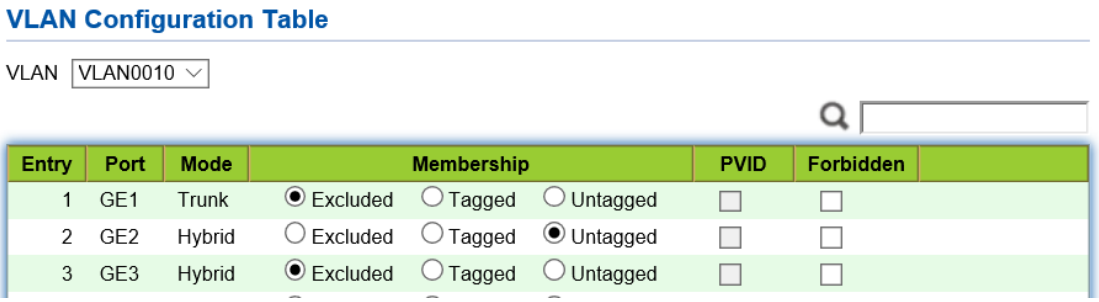
1. 직원이 속한 VLAN을 인식하는 VLAN을 만듭니다. 탐색 트리에서 “VLAN > VLAN > Create VLAN”을 클릭하고 오른쪽의 VLAN 생성 목록에 VLAN10 및 20 을 추가하고 “Apply”하여 완료합니다:



2. 하이브리드 모드에서 스위치 **A** 의 **GE2** 및 **GE3** 인터페이스를 구성합니다 "VLAN > VLAN > Port Setting" 을 클릭하고 하이브리드 모드에서 인터페이스를 수정합니다:



3. 태그가 지정되지 않은 **GE2** 및 **GE3** 를 각각 **VLAN10** 및 **VLAN20** 에 추가합니다 "VLAN > VLAN > VLAN Configuration" 을 클릭하고 목록을 드롭 다운하여 **VLAN10** 및 태그없는 **GE2** 포트를 선택합니다. 동일한 단계에 따라 태그가 지정되지 않은 **GE3** 를 다음과 같이 **VLAN20** 에 추가합니다:



VLAN Configuration Table

VLAN VLAN0020

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	Excluded	Tagged	Untagged		
2	GE2	Hybrid	Excluded	Tagged	Untagged		
3	GE3	Hybrid	Excluded	Tagged	Untagged		
4	GE4	Trunk	Excluded	Tagged	Untagged		

4. 포트에 링크가 필요한 **VLAN** 에 스위치 **B** 의 태그없는 **GE2** 및 **GE3** 인터페이스를 추가합니다. 단계는 **2** 및 **3** 과 유사합니다.
5. 스위치 **A** 의 태그가 지정된 **GE1** 인터페이스를 **VLAN10** 및 **20** 에 추가합니다 "VLAN > VLAN > VLAN Configuration" 을 클릭하고 목록을 드롭 다운하여 **VLAN10** 과 **GE1** 의 태그가 지정된 구성원을 선택합니다. **VLAN20** 을 유사하게 구성하십시오.

VLAN Configuration Table

VLAN VLAN0010

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	Excluded	Tagged	Untagged		

VLAN Configuration Table

VLAN VLAN0020

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	Excluded	Tagged	Untagged		

6. 관련 프로토콜 및 **VLAN. VLAN ID** 는 프로토콜 (패밀리) 유형 및 인터페이스에서 수신 한 메시지의 캡슐화 형식에 따라 할당됩니다. 탐색 트리에서 "VLAN > Protocol VLAN > Protocol Group" 을 클릭하여 프로토콜 그룹에 대한 **2** 개의 규칙을 추가하십시오:

Protocol Group Table

Showing All entries Showing 1 to 2 of 2 entries

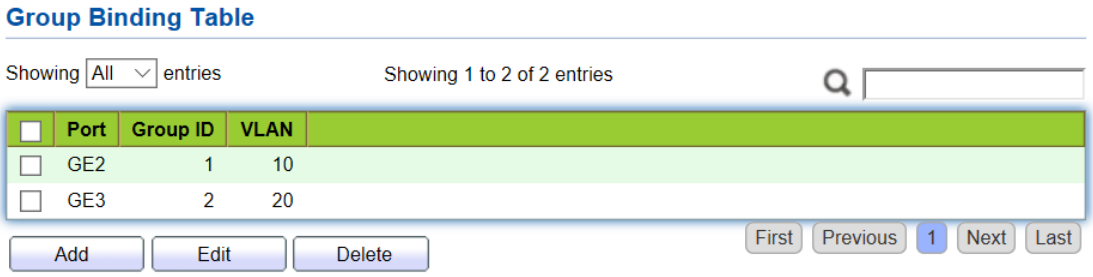
Group ID	Frame Type	Protocol Value
1	Ethernet_II	0x0800
2	Ethernet_II	0x86DD

First Previous 1 Next Last

Add Edit Delete

7. 포트, 프로토콜 그룹 및 **VLAN** 바인딩, "VLAN > Protocol Group > Group Binding"

에서 “Add” 를 클릭하여 **GE2** 및 바인딩 그룹 **ID1** 을 **VLAN10** 에 바인딩하고 **GE3** 및 바인딩 그룹 **ID2** 를 **VLAN20** 에 바인딩합니다:



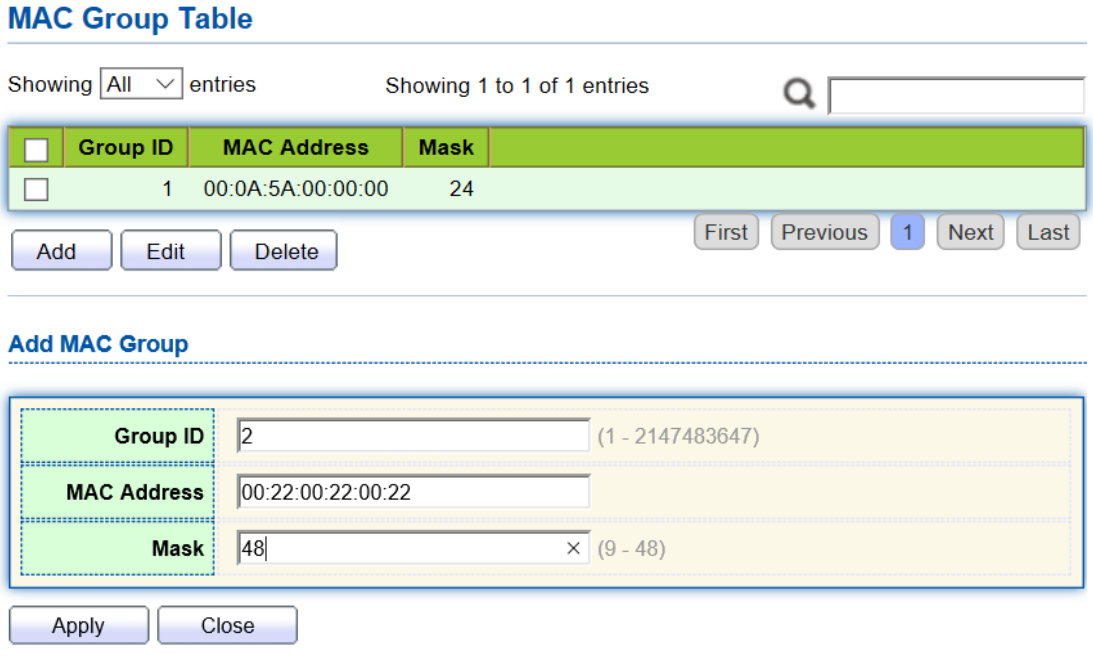
7.4 MAC VLAN

MAC 기반 VLAN 은 네트워크 카드의 MAC 주소에 따라 분할됩니다. 관리자는 스위치가 태그가 지정되지 않은 프레임을 수신하는 경우 추가 될 MAC 주소와 VLAN ID 간의 매핑 체계를 준비합니다.

- 장점 : 터미널 사용자의 물리적 위치가 변경 될 때 VLAN 을 재구성 할 필요가 없으므로 사용자 보안 및 액세스 유연성이 보장됩니다.
- 단점 : 네트워크 카드 및 단순 네트워크 환경이 드물게 교체되는 장면에 적용되며 사전에 멤버가 정의되어 있습니다.

Instructions:

1. 탐색 트리에서 “VLAN > MAC VLAN > MAC Group” 을 클릭하고 다음과 같이 새 **MAC** 그룹을 추가 합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
Group ID	MAC VLAN Group ID
MAC Address	The MAC address to be bound with VLAN
Mask	It indicates the MAC address port. Enter 48 if it is an exact match. Others should be consistent with the masks of IP addresses.

예를 들어 정보 보안 요구 사항이 높은 회사는 **PC** 가 내부 네트워크에만 액세스하도록 허용합니다. 그림과 같이 스위치 **GE1** 은 스위치 **A** 의 업 링크 포트를 연결하고 다운 스트림 포트는 **PC1, 2** 및 **3** 을 연결합니다. 결과적으로 **PC1, 2** 및 **3** 은 스위치 **A** 와 스위치를 통해 내부 네트워크에 액세스 할 수 있지만 다른 **PC** 는 연결할 수 없습니다.

Configuration logic: 다음 단계는 **MAC** 주소를 기반으로 **VLAN** 을 분할하는 데 사용됩니다.

1. 관련 VLAN 을 만듭니다.
2. 올바른 방법으로 이더넷 인터페이스를 VLAN 에 추가합니다.
3. PC1, 2, 3 의 MAC 주소로 VLAN 을 연결합니다.

데이터 준비: 구성 인스턴스에 대해 다음 데이터를 준비해야 합니다:

- 스위치에서 **GE1 PVID** 를 **100** 으로 설정합니다.
- 스위치에서 태그가 지정되지 않은 방식으로 **VLAN10** 에 액세스하도록 **GE1** 을 설정합니다.
- 스위치에서 태그가 지정된 방식으로 **VLAN10** 에 액세스하도록 **GE2** 를 설정합니다.
- 기본적으로 스위치 **A** 인터페이스를 설정합니다. 즉, 모든 인터페이스가 태그가 지정되지 않은 방식으로 **VLAN1** 에 추가됩니다.
- **PC1, 2, 3** 의 **MAC** 주소를 **VLAN10** 과 연결합니다.

MAC 주소를 기반으로 **VLAN** 분할에 대한 네트워킹 다이어그램을 그립니다

Instructions:

1. 직원이 속한 **VLAN** 을 인식하는 **VLAN** 을 만듭니다. 탐색 트리에서 “VLAN > VLAN > Create VLAN” 을 클릭하고 오른쪽의 **VLAN** 생성 목록에 **VLAN10** 을 추가하고 “Apply” 하고 다음과 같이 완료합니다:

VLAN Table

Showing All entries Showing 1 to 3 of 3 entries

	VLAN	Name	Type	VLAN Interface State
○	1	default	Default	Disabled
○	10	VLAN0010	Static	Disabled
○	100	VLAN0100	Static	Disabled

First Previous 1 Next Last

Edit Delete

2. **VLAN10** 의 태그가 지정되지 않은 구성원 역할을하도록 **PVID** 가 **100** 인 하이브리드 모드에서 스위치의 **GE1** 을 구성합니다. **VLAN10** 의 태그가 지정된 멤버로 작동하도록 트렁크 모드에서 **GE2** 를 구성합니다.

Port Setting Table

	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Hybrid	100	All	Enabled	Disabled	0x8100
☐	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
○	1	GE1	Hybrid	1U, 10U, 100P	1U, 10U, 100P
○	2	GE2	Trunk	1UP, 10T	1UP, 10T
○	3	GE3	Trunk	1UP	1UP

3. 기본적으로 스위치 **A** 의 인터페이스를 구성합니다. 즉, 모든 인터페이스가 태그가 지정되지 않은 방식으로 **VLAN1** 에 액세스합니다. **PC1, 2, 3** 의 **MAC** 주소를 **VLAN10** 과 연결합니다. 탐색 트리에서 “VLAN > MAC VLAN > MAC Group” 을 클릭하고 **PC1 (0022-0022-0022), PC2 (0033-0033-0033)** 및 **PC3 (0044-0044-0044)**의 **MAC** 주소를 입력합니다., 다음과 같이 **48** 비트 정확히 일치 마스크를 사용합니다:

MAC Group Table

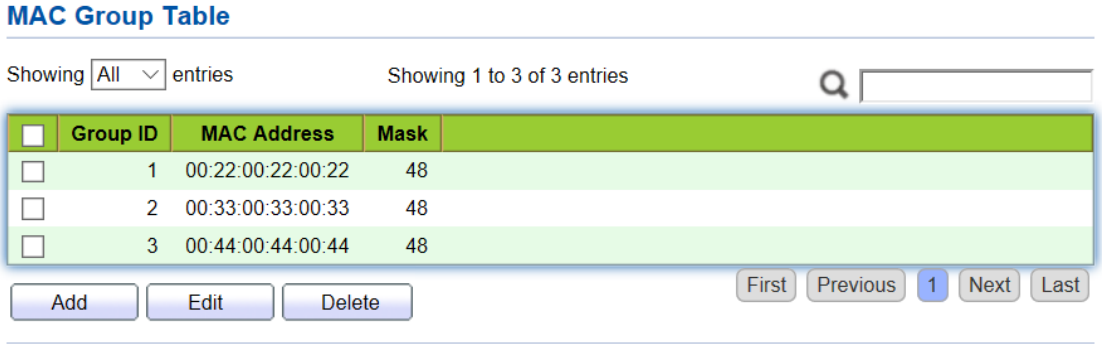
Showing All entries Showing 1 to 3 of 3 entries

	Group ID	MAC Address	Mask
☐	1	00:22:00:22:00:22	48
☐	2	00:33:00:33:00:33	48
☐	3	00:44:00:44:00:44	48

First Previous 1 Next Last

Add Edit Delete

4. 탐색 트리에서 "VLAN > MAC VLAN > Group Binding" 을 클릭하고, "**Add**" 를 클릭하여 하이브리드 포트만, 바인딩 할 **MAC** 그룹 **ID** 및 지정된 **VLAN ID** 를 선택합니다. "Apply" 하고 완료합니다:



5. 구성을 확인합니다.
오직 PC1,2,3 만 내부 네트워크에 액세스할 수 있습니다.

7.5 Surveillance VLAN

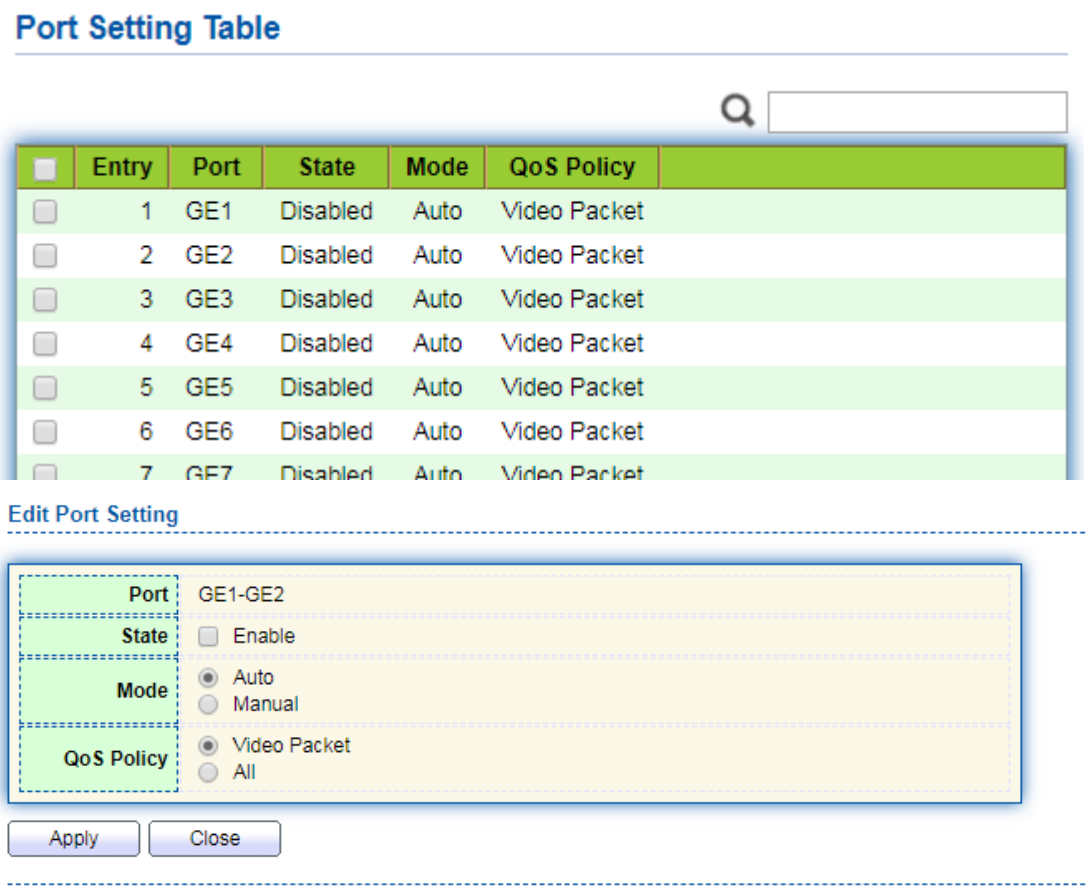
Surveillance VLAN 은 주로 비디오 스트림 패킷에 사용된다. 전송 프로세스에서 그러한 패킷의 우선순위를 보장하기 위해, 일반 패킷보다 높은 우선순위를 갖는다.

Instructions:
1. 탐색 트리에서 "VLAN > Surveillance VLAN > Property" 를 선택한다.



구성 품목	설명
State	Surveillance VLAN 을 활성화 합니다.
VLAN	VLAN 1 에서 4,094 까지 추가된 VLAN ID(예: 1-3, 5, 7, 9)를 지정합니다. 다른 VLAN 은 링크가 필요한 포트에 태그가 지정되지 않은 방식으로 추가되어야 한다.
CoS / 802.1p	VOICE VLAN 메시지 우선 순위 재정의 여부를 설정합니다.

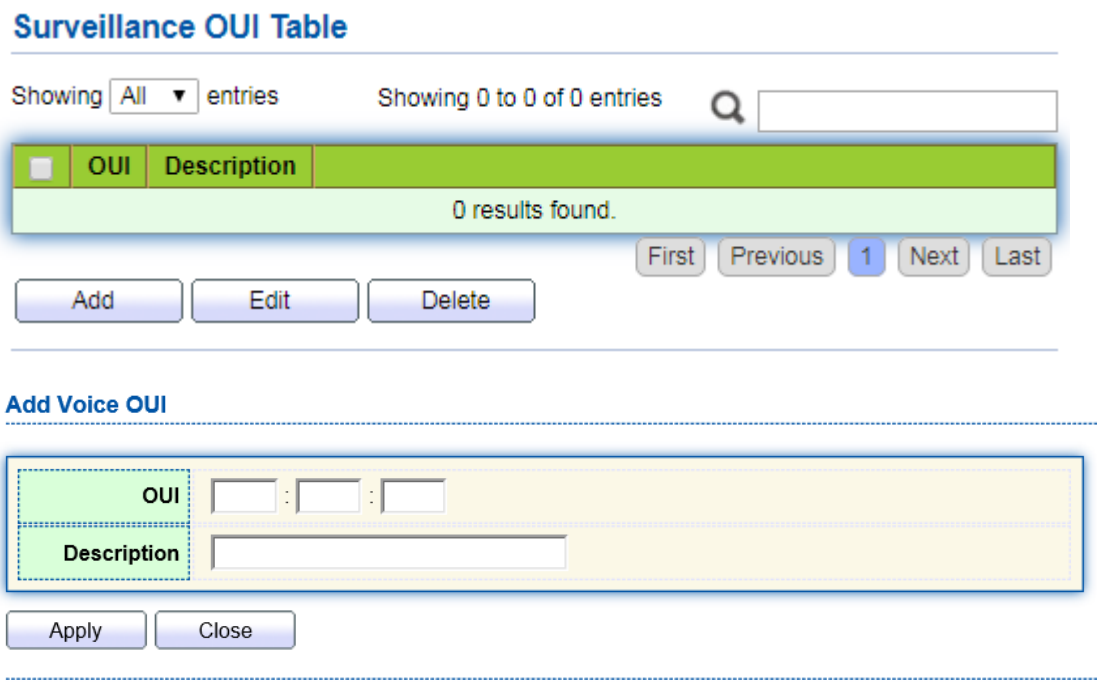
Remarking	
Aging Time	Table aging time



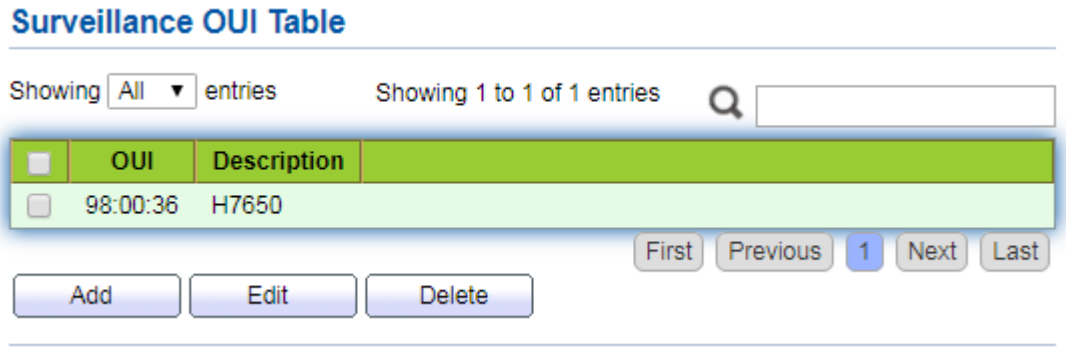
구성 항목은 다음과 같습니다.

구성 항목	설명
Port	활성화된 포트
State	Surveillance VLAN 을 활성화 합니다.
Mode	Surveillance VLAN port 모드를 자동 또는 수동으로 설정합니다.
QoS Policy	QoS 에 영향 받게될 메시지를 선택합니다.

2. 탐색 트리에서 “VLAN > Surveillance VLAN > Surveillance OUI”을 클릭해서, OUI of Surveillance VLAN OUI 의 주소 세그먼트를 설정합니다:



3. 해당 구성 항목을 작성합니다.
4. 다음과 같이 “Apply” 합니다.



7.6 GVRP

GVRP VLAN 등록 프로토콜은 일반 속성 등록 프로토콜의 응용 프로그램으로 802.1Q 호환 VLAN 프루닝 기능과 802.1Q 트렁크 포트 트렁크 포트에서 동적 VLAN 설정을 제공합니다.

GVRP 스위치는 VLAN 구성 정보를 서로 교환하고 불필요한 브로드 캐스트 및 알려지지 않은 유니 캐스트 트래픽을 차단하며 802.1Q 트렁크를 통해 연결된 스위치에서 동적으로 VLAN 을 생성 및 관리 할 수 있습니다.

GID 및 GIP 는 GVRP 에서 사용되며 각각 GARP 기반 애플리케이션에 대한 일반적인 상태 메커니즘 설명 및 정보 배포 메커니즘을 제공합니다. GVRP 는 802.1Q 트렁크 링크에서만 실행됩니다. GVRP 는 트렁크 링크를 차단하여 활성 VLAN 만 트렁크 연결에서 전송되도록합니다. GVRP 가 VLAN 을 트렁크 라인에

추가하기 전에 먼저 스위치에서 결합 정보를 수신합니다. GVRP 업데이트 정보 및 타이머를 변경할 수 있습니다. GVRP 포트에는 VLAN 을 조정하는 방법을 제어하는 다양한 작동 모드가 있습니다. GVRP 는 VLAN 데이터베이스 용 VLAN 을 동적으로 추가하고 관리 할 수 있습니다.

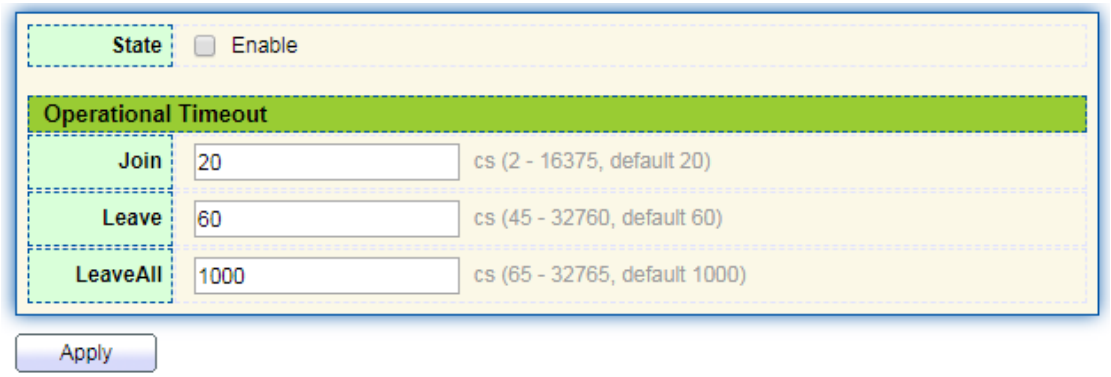
GVRP 는 장치 간의 VLAN 정보 전파를 지원합니다. GVRP 에서 스위치의 VLAN 정보는 수동으로 구성 할 수 있으며 네트워크의 다른 모든 스위치는 VLAN 을 동적으로 이해할 수 있습니다. 터미널 노드는 모든 스위치에 액세스하고 필요한 VLAN 에 연결할 수 있습니다. GVRP 를 사용하려면 GVRP 호환 네트워크 인터페이스 카드 (NIC)를 설치해야합니다. GVRP 호환 NIC 를 구성하여 필요한 VLAN 에 연결 한 다음 GVRP 지원 스위치에 액세스 할 수 있습니다. NIC 와 스위치 간의 통신 연결이 설정되고 NIC 와 스위치간에 VLAN 연결이 실현됩니다.

7.6.1 Property

글로벌 및 포트 설정

Instructions:

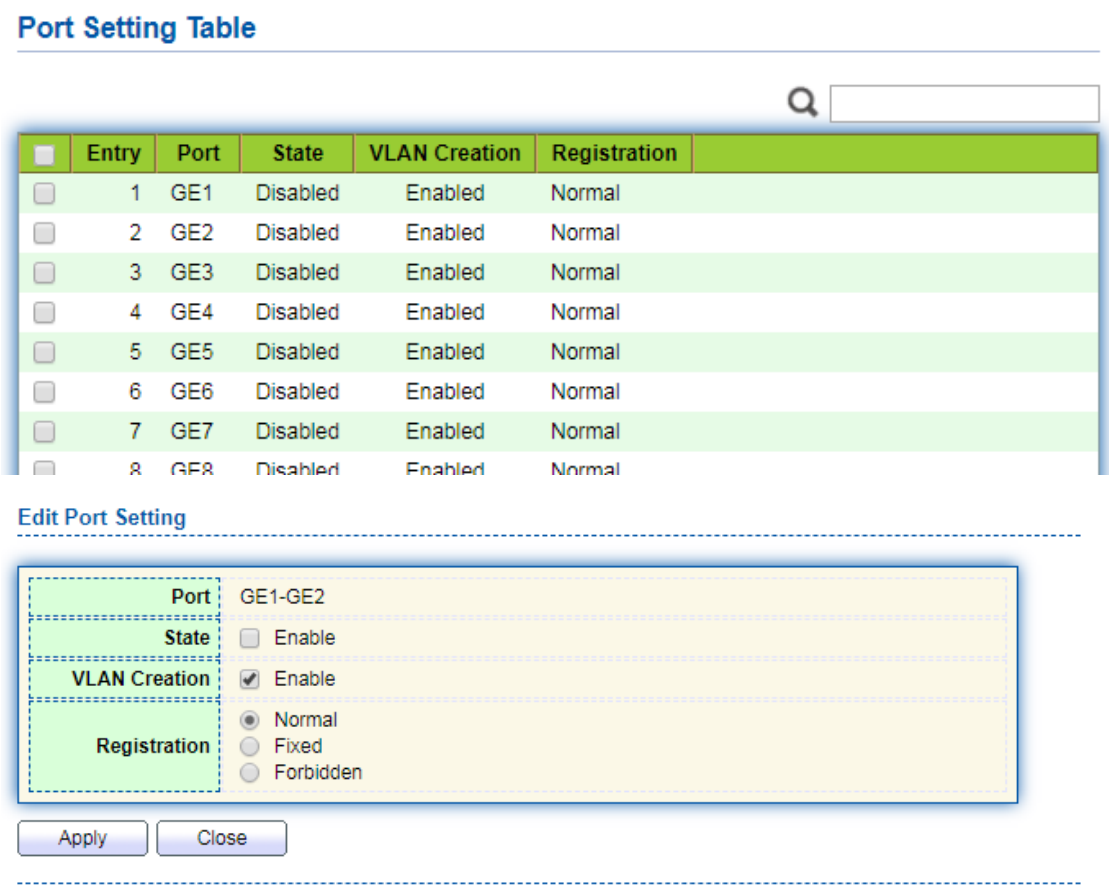
1. 탐색 트리에서 “VLAN > GVRP > Property”을 클릭합니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
State	GVRP 기능의 활성화 상태
Join	1-20cs 범위의 값(1/100 초 단위). 기본값은 20cs 입니다.
leave	60-300cs 범위의 값(100 분의 1 초 단위). 기본값은 60cs 입니다.
LeaveAll	1000-5000cs 범위의 값(100 분의 1 초 단위). 기본값은 1000cs 입니다.

2. 탐색 트리에서 “VLAN > GVRP > Property”를 클릭하고, 포트를 선택한 다음 “Edit”를 클릭합니다:



구성 항목은 다음과 같습니다.

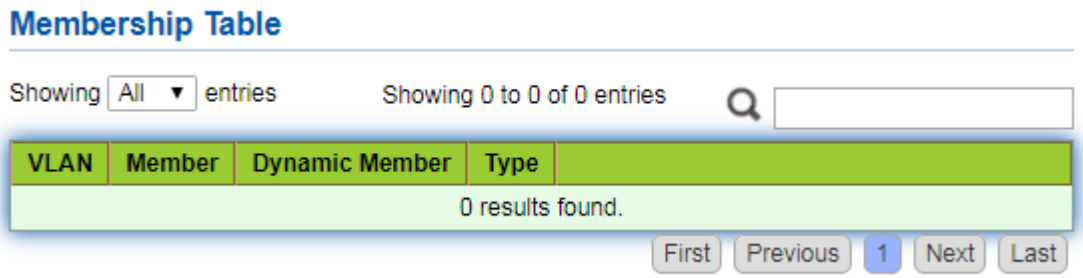
구성 항목	설명
Port	포트 목록
State	GVRP 기능의 활성화 여부
VLAN Creation	VLAN 자동 생성 활성화 여부
Registration	GVRP 의 3 가지 등록 모드 Normal : 동적 VLAN 이 포트에 등록하고 정적 VLAN 및 동적 VLAN 의 선언 메시지를 동시에 보낼 수 있습니다. Fixed : 동적 VLAN 은 포트에 등록 할 수 없으며 정적 VLAN 선언 메시지만 전송됩니다. Forbidden : 동적 VLAN 은 포트에 등록 할 수 없습니다. 동시에 포트에서 vlan1 을 제외한 모든 VLAN 이 삭제되고 vlan1 선언 메시지만 전송됩니다.

7.6.2 Membership

GVRP dynamic member 정보를 확인합니다.

Instructions:

1. 탐색 트리에서 “VLAN > GVRP > Membership”을 클릭합니다.

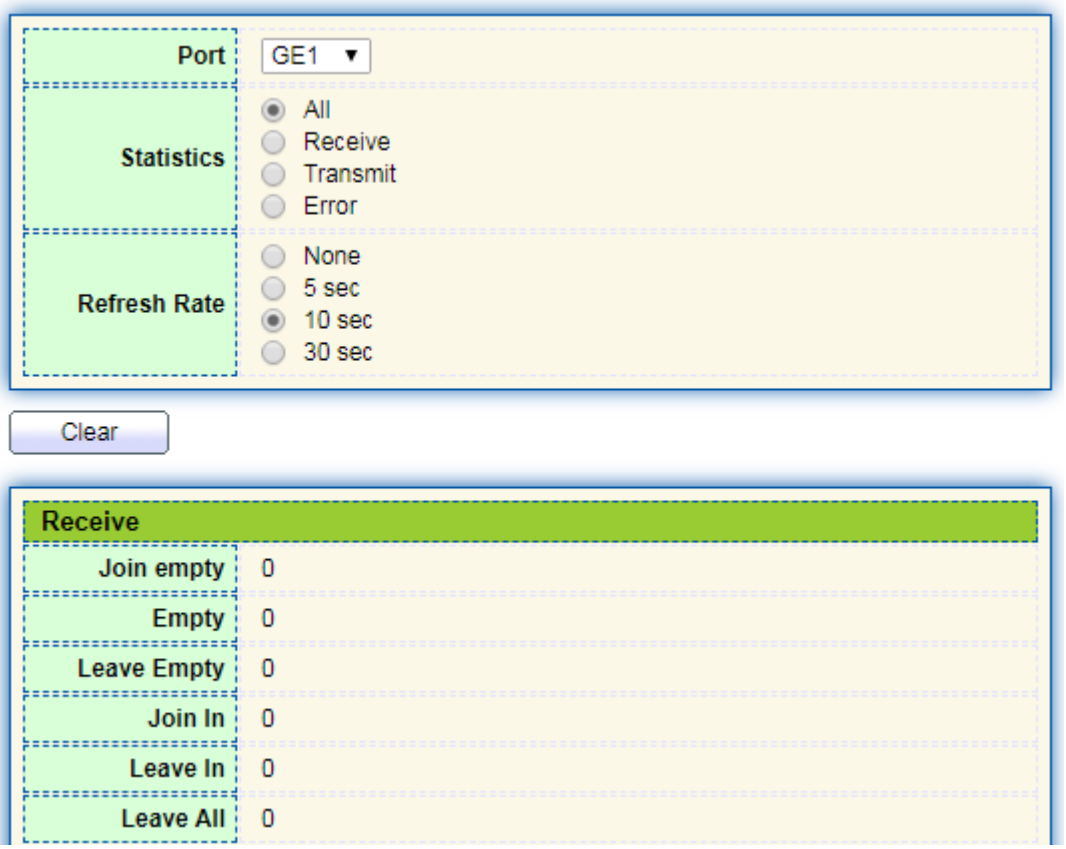


7.6.3 Statistics

포트 GVRP message 통계를 확인합니다.

Instructions:

1. 탐색 트리에서 “VLAN > GVRP > Statistics”를 클릭합니다.



8 MAC Address Table

이더넷 스위치는 주로 데이터 링크 계층의 목적에 따라 포워딩하도록 혁신되었습니다. 즉, **MAC** 주소는 용도에 따라 해당 포트로 메시지를 전송합니다. **MAC** 주소 포워딩 테이블은 **L2** 메시지의 고속 포워딩의 기반이되는 **MAC** 주소와 포워딩 포트를 나타내는 **L2** 테이블입니다.

MAC 주소 전달 테이블에는 다음 데이터가 포함됩니다:

- 대상 **MAC** 주소
- 포트에 속한 **VLAN ID**
- 이 장치의 포워딩 수신 번호

MAC 주소 테이블 정보에 따라 두 가지 메시지 전달 유형이 있습니다:

- Unicast mode: **MAC** 주소 전달 테이블에 대상 **MAC** 주소와 해당 항목이 포함되어있는 경우 스위치가 테이블의 송신에서 메시지를 직접 전송합니다.
- Broadcast mode: 스위치가 목적지 주소가 F- 비트로 가득 찬 메시지를 수신하거나 전달 테이블에 MAC 목적지 주소에 해당하는 항목이없는 경우 스위치는 이러한 방식으로 수신 포트를 제외한 모든 포트로 메시지를 전달합니다.

8.1 Dynamic Address

MAC 주소의 에이징 시간 및 테이블 정보는이 페이지에서 구성하고 확인할 수 있습니다.

MAC 주소 테이블은 네트워크 변경을 수용하기 위해 지속적인 업데이트가 필요합니다. 수명 (예: aging time). 에 의해 제한되는 항목을 자동으로 생성합니다. 만료 후 새로 고쳐지지 않은 항목은 삭제됩니다. 만료 전에 레코드를 새로 고치면 항목의 에이징 시간이 다시 계산됩니다.

적절한 에이징 시간은 **MAC** 주소의 에이징 목표를 달성하는 데 도움이됩니다. 에이징 시간이 부족하면 대상 **MAC** 주소의 패킷을 검색하기 위해 많은 수의 스위치가 브로드 캐스트되어 스위치 성능에 영향을 미칠 수 있습니다.

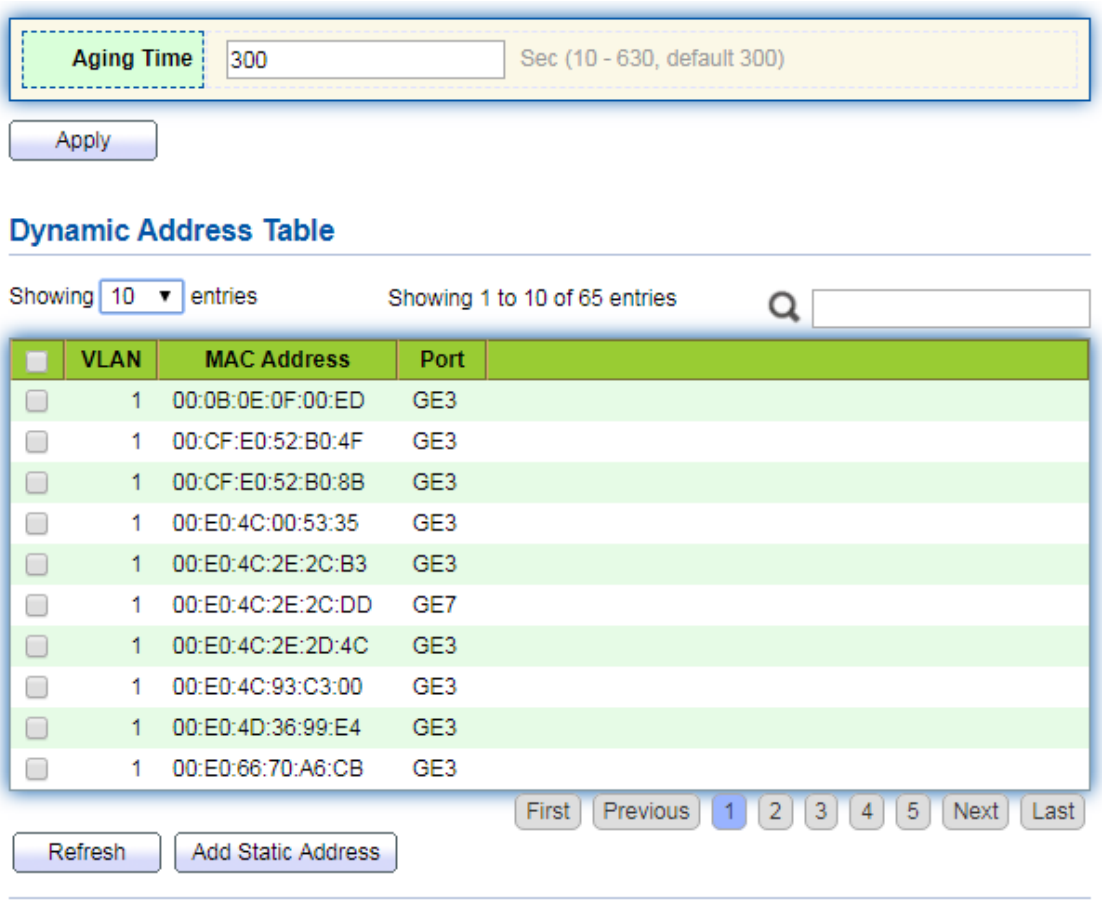
시간이 너무 오래 걸리면 스위치가 오래된 **MAC** 주소 항목을 저장하여 전달 리소스를 고갈시키고 네트워크 변경을 기반으로 전달 테이블을 업데이트하지 못할 수 있습니다.

스위치는 너무 짧은 에이징 시간으로 인해 유효한 **MAC** 주소 테이블 항목을 제거하여 전달 효율성을 떨어 뜨릴 수 있습니다.

일반적으로 권장되는 에이징 시간은 기본적으로 **300** 초입니다.

aging time 세팅 방법:

1. 구성 및 디스플레이 인터페이스에 대한 탐색 트리에서 “MAC Address Table > Dynamic Address” 를 클릭합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
MAC Aging Time	MAC address 의 에이징 타입을 입력합니다.

2. 해당 항목을 입력합니다.
3. “Apply” 하고 마칩니다.

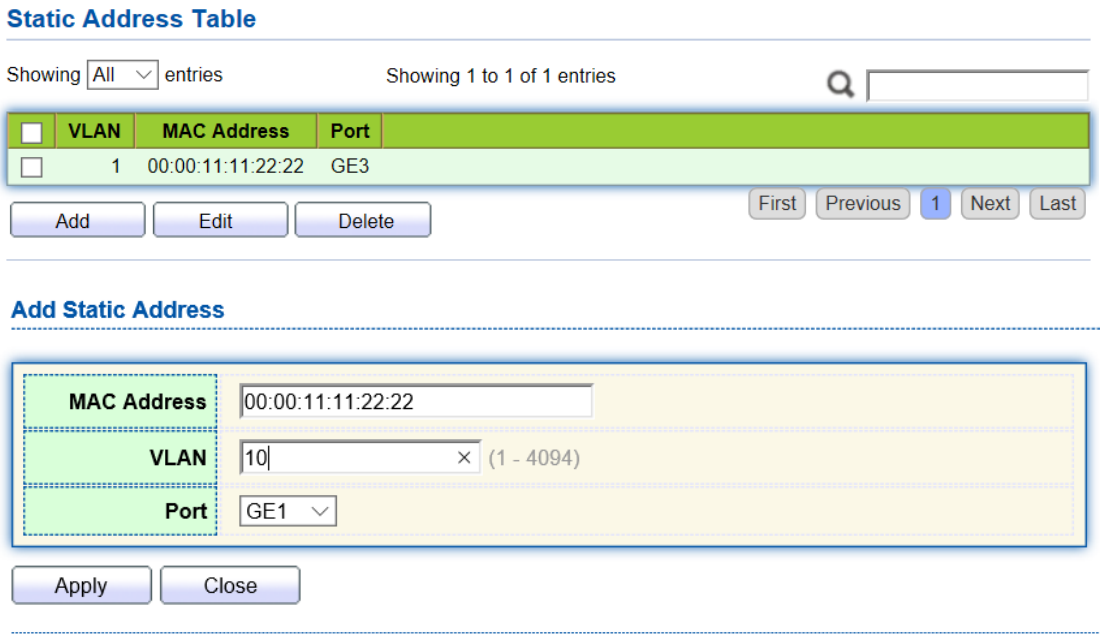
MAC Table 은 스위치에 의해 학습 된 **MAC** 주소, **VLAN** 번호, 수신/송신(**Ingress / Egress)** 정보 등을 저장합니다. 데이터를 전달할 때 대상 **MAC** 주소 및 이더넷 프레임의 **VLAN** 번호 쿼리 테이블에 따라 장치 **Egress** 를 빠르게 찾습니다.

MAC 주소 표에 대한 지침을 확인하십시오(3 장 3.3 MAC Address Table 참고)

8.2 Static Address

정적 테이블은 사용자가 수동으로 구성하고 에이징되지 않는 각 인터페이스 보드에 배포됩니다.

Instructions:
1. 탐색 트리에서 "MAC Address Table > Static Address"를 클릭합니다.



구성 항목은 다음과 같습니다.

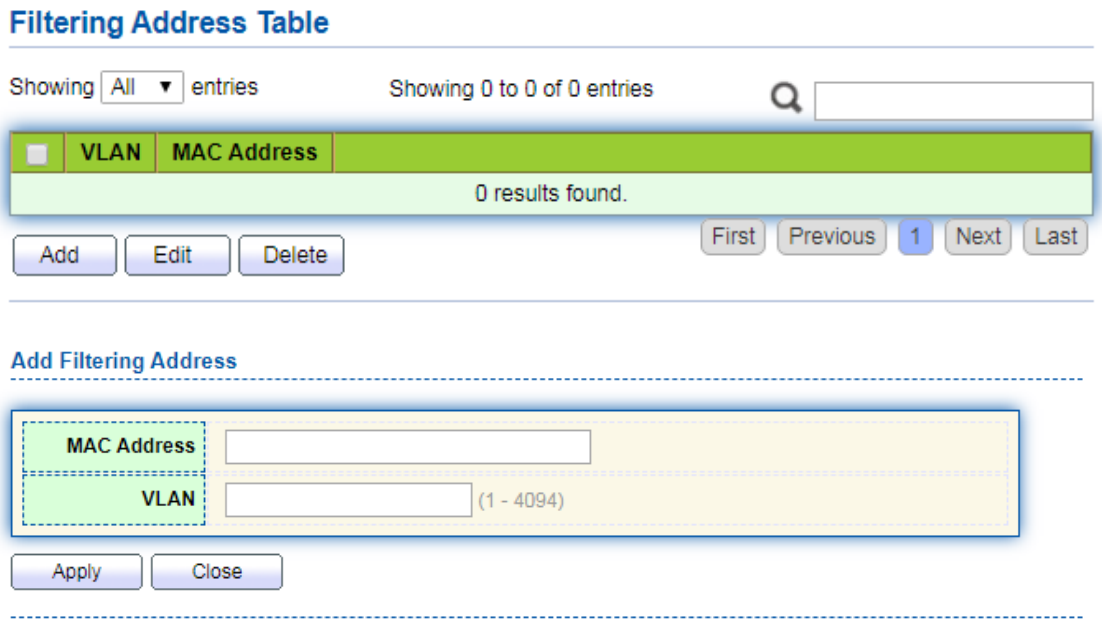
구성 항목	설명
MAC	필수, 새 **MAC** 주소 입력 (예 : **HH : HH : HH : HH : HH : HH**)
VLAN	필수, **VLAN ID** 지정
Port	필수, 인터페이스 유형을 선택하고 인터페이스 이름을 입력하십시오 반드시 구성된 **VLAN** 의 구성원 포트여야 합니다.

2. 구성 항목을 입력하고, "Apply"하여 완료합니다.

8.3 Filtering Address

설정에 따라 조건에 일치하는 데이터 프레임을 폐기합니다.

Instructions:
1. 탐색 트리에서 "MAC Address Table > Filtering Address"을 클릭합니다.



구성 항목은 다음과 같습니다.

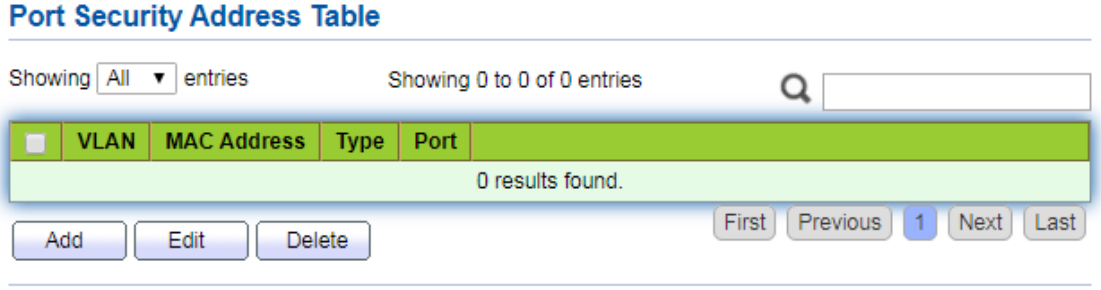
구성 항목	설명
MAC Address	필터링할 MAC Address 를 설정합니다.
VLAN	MAC address 의 VLAN

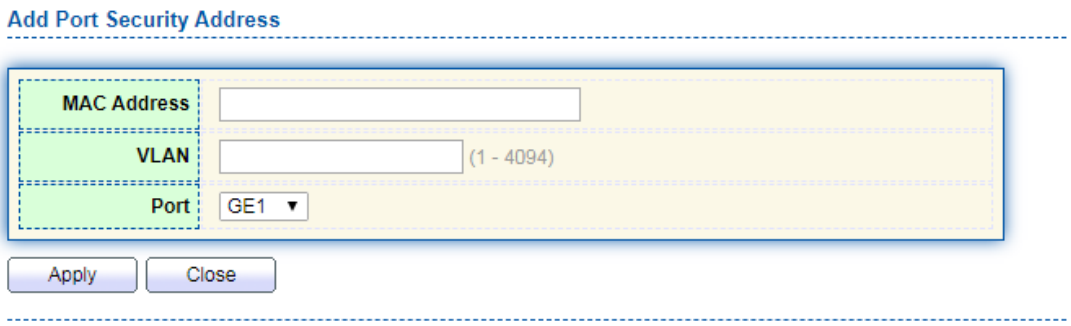
8.4 Port Security Address

MAC 주소가 Security Address 로 설정된 경우, 포트는 Security Address 의 데이터 프레임만 통과하도록 허용하고, 나머지는 폐기합니다.

Instructions:

1. 탐색 트리에서 “MAC Address Table > Port Security Address”을 클릭합니다:





구성 항목은 다음과 같습니다..

구성 항목	설명
MAC Address	보안 설정할 MAC Address
VLAN	MAC address 의 VLAN
Port	Port security 기능을 적용할 포트

9 Spanning Tree

이더넷 스위칭 네트워크에서 링크 백업 및 네트워크 안정성을 위해 중복 링크가 자주 사용됩니다. 그러나 이러한 링크는 스위칭 네트워크에서 루프를 생성하여 브로드 캐스트 스톰, 불안정한 MAC 주소 목록 및 기타 오류를 유발하여 사용자의 통신 품질을 악화 시키거나 통신을 방해 할 수도 있습니다. 그 결과 STP (Spanning Tree Protocol)가 나타납니다.
IEEE 802.1D 에 정의 된 원래 STP 에서 IEEE 802.1W 에 정의 된 RSTP (Rapid Spanning Tree Protocol), IEEE 802.1S 에 정의 된 MSTP (Multiple Spanning Tree Protocol)에 이르기까지 다른 프로토콜의 개발과 마찬가지로 STP 는 계속 업그레이드됩니다.
MSTP 는 RSTP 및 STP 와 호환되는 반면 RSTP 는 STP 와 호환됩니다. 이 세 가지 프로토콜 간의 대비가 표에 나와 있습니다.

3 가지 프로토콜의 대비

STP	특성	응용
STP	스톰과 중복 백업을 브로드 캐스트하는 솔루션으로 루프를 제거하는 트리입니다. 천천히 수렴합니다.	모든 **VLAN** 은 사용자 또는 비즈니스 흐름에서 차별없이 공유 될 수 있습니다.
RSTP	스톰 및 중복 백업을 브로드 캐스트하는 솔루션으로 루프를 제거하는 트리입니다. 빠르게 수렴합니다	

MSTP	스톰 및 중복 백업을 브로드 캐스트하는 솔루션으로 루프를 제거하는 트리입니다. 빠르게 수렴합니다. 스패닝 트리는 **VLAN** 간의로드 균형을 조정합니다. 다른 **VLAN** 의 흐름은 경로에 따라 전달됩니다	부하 공유를 위해 사용자와 비즈니스 흐름을 구분합니다. 서로 다른 **VLAN** 은 별도의 스패닝 트리를 통해 흐름을 전달합니다.

STP 가 적용된 후 토폴로지를 사용하여 루프를 계산하여 다음 목표를 달성할 수 있습니다:

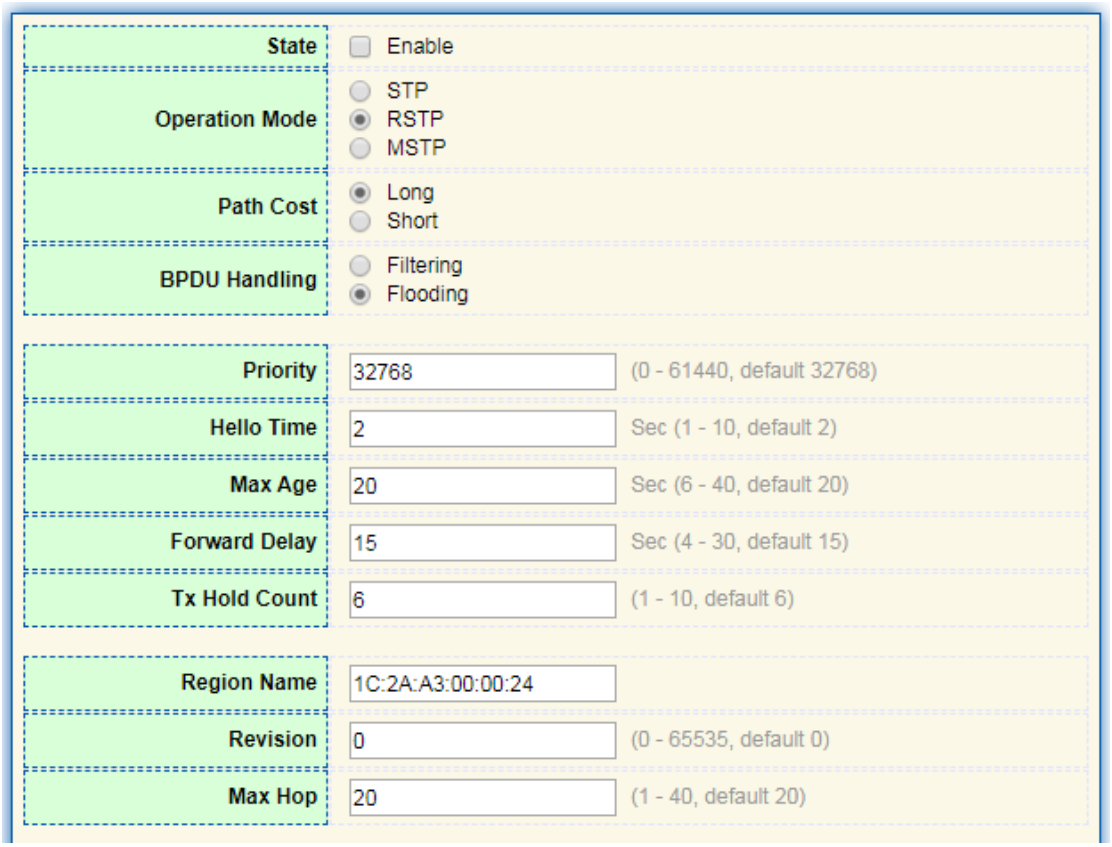
- Loop elimination: 중복 링크를 차단하여 가능한 통신 루프를 제거합니다.
- Link backups: 활성 경로가 실패할 경우 네트워크 연결을 복원하기 위해 중복 링크를 활성화합니다.

9.1 Property

STP 전역 매개 변수를 구성합니다. 특정 네트워크 환경에서는 최상의 성능을 얻기 위해 일부 장치의 **STP** 매개 변수를 조정해야합니다.

Instructions:

1. 탐색 트리에서 “Spanning Tree > Property”을 클릭합니다:



구성 항목은 다음과 같습니다.

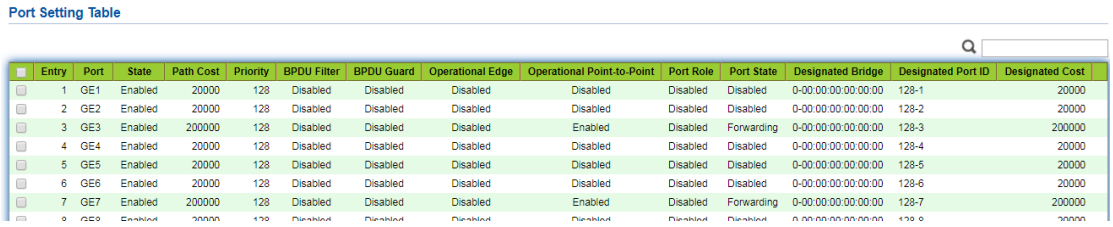
구성 항목	설명
State	스위치 대신 스패닝 트리를 활성화하도록 기본적으로 선택되어 있습니다.
Operation Mode	세 가지 모드, 즉 **STP, RSTP** 및 **MSTP** 를 사용할 수 있습니다.
Path Cost	**Long** 모드 및 **Short** 모드
BPDU Handling	장치에서 수신 한 **BPDU** 메시지를 처리하는 방법
Priority	포트 우선 순위
Hello Time	**Hello** 메시지 간격
Max Age	최대 aging time
Forward Delay	앞으로 지연 시간
Tx Hold Count	초당 최대 패킷 전송 수를 제한하는 데 사용되는 Tx-Hold-Count 를 지정합니다.
Region Name	**MST** 도메인 이름. 스위치 마스터 보드는 기본적으로 **MAC** 주소를 설정합니다. **MST** 도메인의 **VLAN** 매핑 테이블 및 **MSTP** 의 개정 수준과 함께 스위치 도메인 이름은 자신이 속한 도메인을 공동으로 결정합니다.
Revision	MSTP revision number
Max Hop	BPDU 가 삭제되기 전의 MSPT 영역의 홉 수를 지정합니다.

2. 해당 설정 항목을 입력합니다.
3. “Apply” 하고 완료합니다.

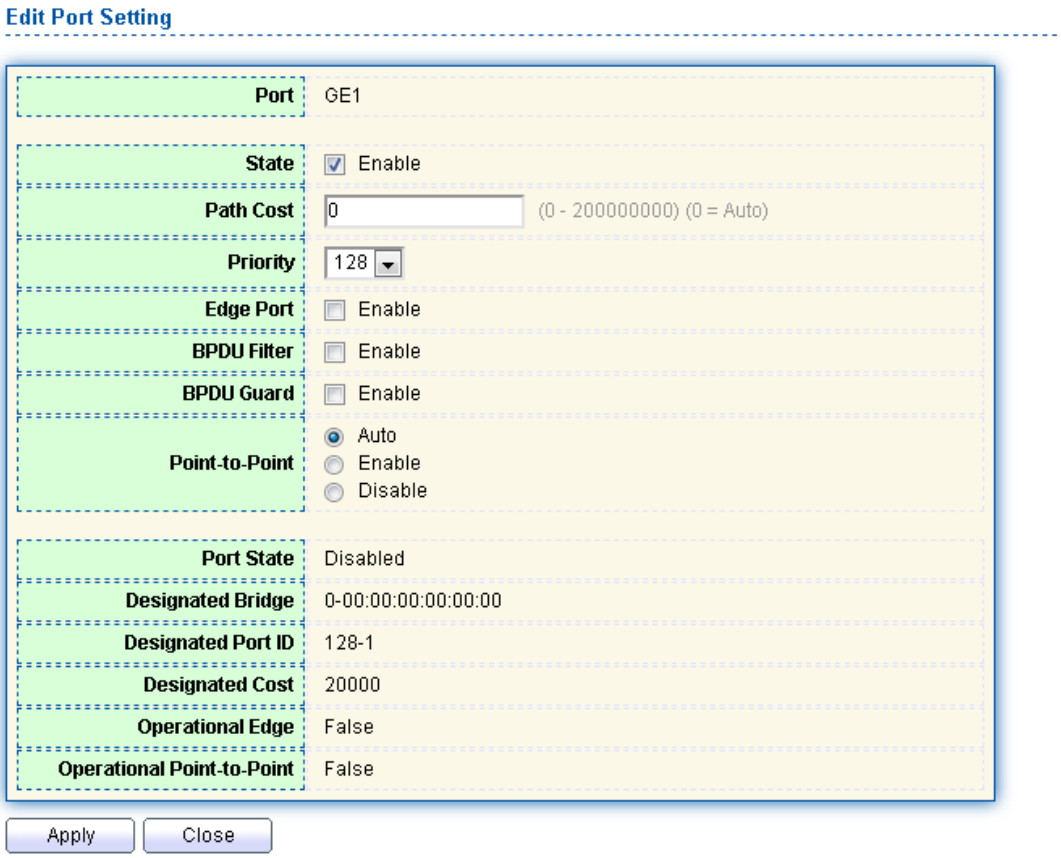
9.2 Port Setting

특정 네트워크 환경에서 일부 장치의 **STP** 매개 변수는 최상의 성능을 위해 조정되어야합니다.

1. 탐색 트리에서 “Spanning Tree > Port Setting” 을 클릭하고, 포트를 선택한 다음 “Edit” 를 선택하여 속성을 설정합니다:


Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
3	GE3	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-3	200000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-7	200000



구성 항목은 다음과 같습니다.

구성 항목	설명
Port	속성을 구성 할 포트 번호
State	**STP** 활성화 여부
Path Cost	Enter the path cost value of the interface Use IEEE 802.1t Standard with the value ranging from 0 to 200,000,000
Priority	포트 우선 순위를 설정합니다(작은 값이 높은 우선 순위). 인터페이스 우선 순위는 지정된 MSTI 의 인터페이스 역할에 영향을 줍니다. 다른 MSTI 에서 사용자는 동일한 인터페이스에 대한 우선 순위를 구성할 수 있습니다. 결과적으로 서로 다른 VLAN 의 흐름이 물리적 링크를 따라 전달되어 VLAN 로드 공유를 달성할 수 있습니다. MSTP 는 인터페이스 역할을 다시 계산하고 우선 순위가 변경되면 해당 상태를 마이그레이션합니다.
Edge Port	다른 스위치나 네트워크 세그먼트가 아니라 에지 포트를 사용자 터미널에 직접 연결해야합니다. 토폴로지 변경으로 인해 루프가 생성되지 않으므로 순방향 상태로 빠르게 전환 할 수 있습니다. 구성중인 에지 포트는 **STP** 에 의해 순방향 상태로 빠르게 전환 될 수 있습니다. 이를 위해서는 사용자 터미널에 직접 연결된

	이더넷 포트를 에지 포트로 구성하는 것이 좋습니다.
BPDU Filter	**BPDU** 필터 활성화 여부
BPDU Guard	**BPDU Guard** 를 활성화하거나 비활성화합니다. 기본적으로 선택되어 있지 않습니다. **BPDU Guard** 가 활성화 된 경우 장치는 **BPDU** 를 수신하는 인터페이스를 종료하고 **NMS** 에 알립니다. 이러한 인터페이스는 네트워크 관리자 만 수동으로 복원 할 수 있습니다
Point-to-Point	활성화, 종료 및 자동 모드를 선택합니다. Auto mode: 기본 자동 검사와 지점 간 링크 간의 연결 상태를 나타냅니다. Enabled mode: 특정 포트가 지점 간 링크에 연결되어 있음을 나타냅니다. Shutdown mode: 특정 포트가 지점 간 링크 연결에 실패했음을 나타냅니다.

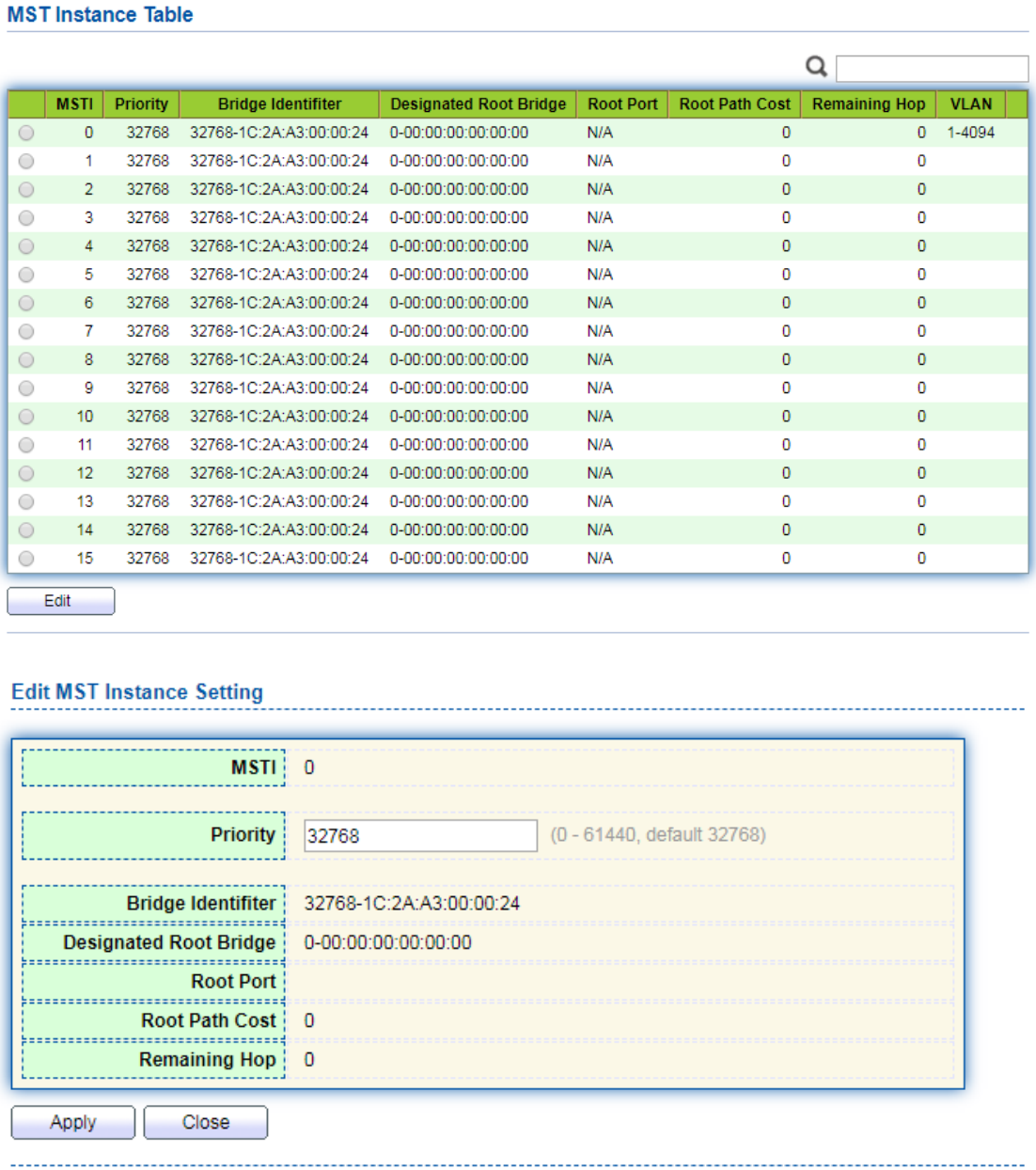
3. 해당 구성 항목을 입력합니다.
4. “Apply” 하고 완료합니다.

9.3 MST Instance

스위칭 네트워크는 **MSTP** 에 의해 여러 도메인으로 분할되며 각 도메인 내에 독립적인 스패닝 트리가 형성됩니다. 각 스패닝 트리를 **MSTI (Multiple Spanning Tree Instance)**라고하고 각 도메인을 **MST** 영역 : 다중 스패닝 트리 영역이라고합니다.

인스턴스는 통신 비용과 리소스 사용률을 줄이는 **VLAN** 그룹입니다. 토폴로지로 독립적으로 계산 된 각 인스턴스는로드 균형을 맞출 수 있습니다. 토폴로지가 동일한 **VLAN** 은 동일한 인스턴스에 매핑 될 수 있으며 해당 **MSTP** 인스턴스의 포트 상태에 따라 전달됩니다.
간단히 말해서 지정된 **MST** 인스턴스에 매핑 된 하나 이상의 **VLAN** 이 한 번에 스패닝 트리에 배포됩니다.

Instructions:
1. 탐색 트리에서 “Spanning Tree > MST Instance”을 선택하고, “Edit”를 클릭하여 MST Instance 를 수정합니다:



구성 항목은 다음과 같습니다.

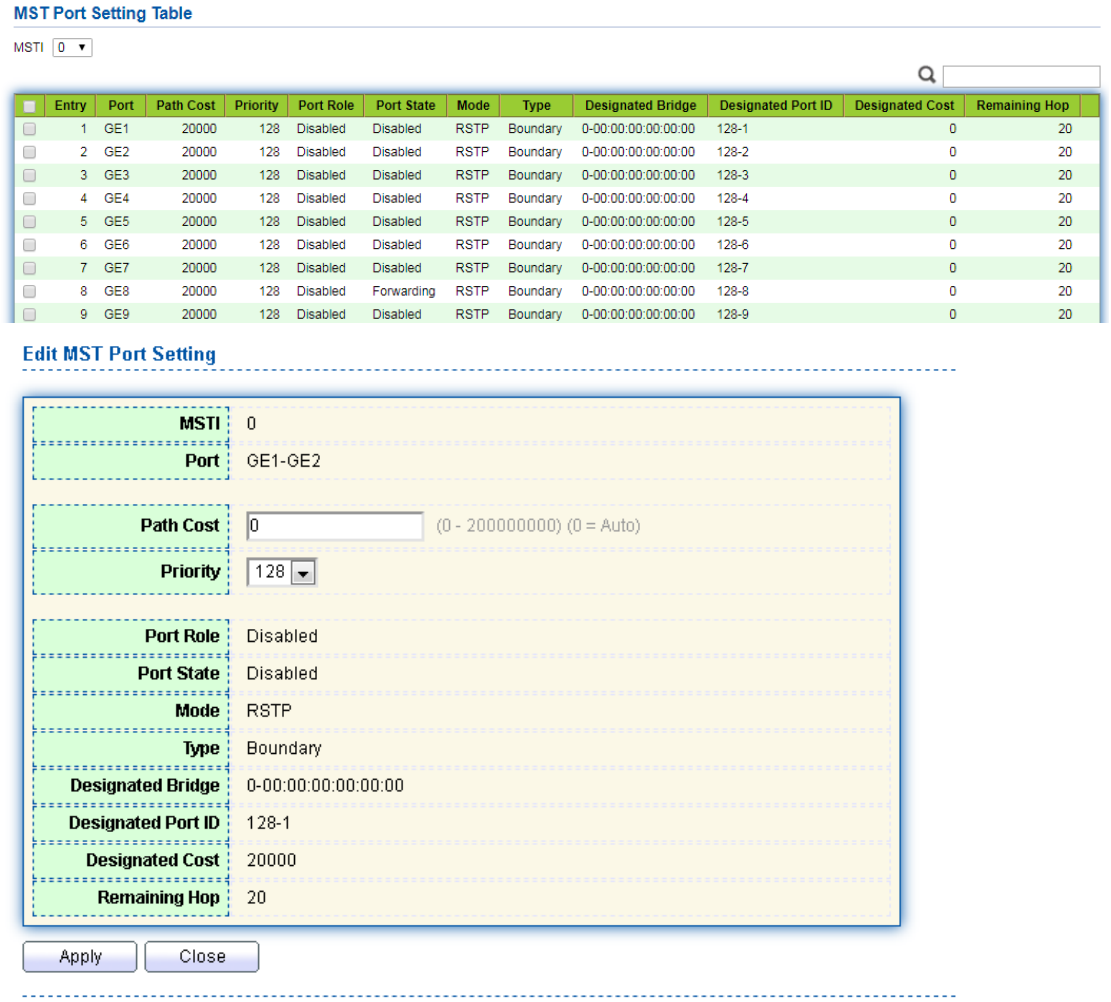
구성 항목	설명
MSTI	스패닝 트리의 인스턴스 번호는 **0** 에서 **15** 까지입니다
VLAN	인스턴스에서 매핑 된 **VLAN** 번호
Priority	지정된 인스턴스에 대해 **4,096** 의 배수 우선 순위를 **0** 에서 **65,535** 범위로 설정하고 기본값은 **32,768** 입니다.

2. 해당 구성 항목을 입력합니다.
3. “Apply” 하고 다음과 같이 마칩니다.

9.4 MST Port Setting

Instructions:

1. 내비게이션 트리에서 “Spanning Tree > MST Port Setting” 을 클릭하고, 장치의 모든 포트 목록에서 수정할 포트를 확인하고 “Edit” 를 선택하면 다음과 같이 세부 구성 인터페이스로 들어갑니다:



구성 항목은 다음과 같습니다.

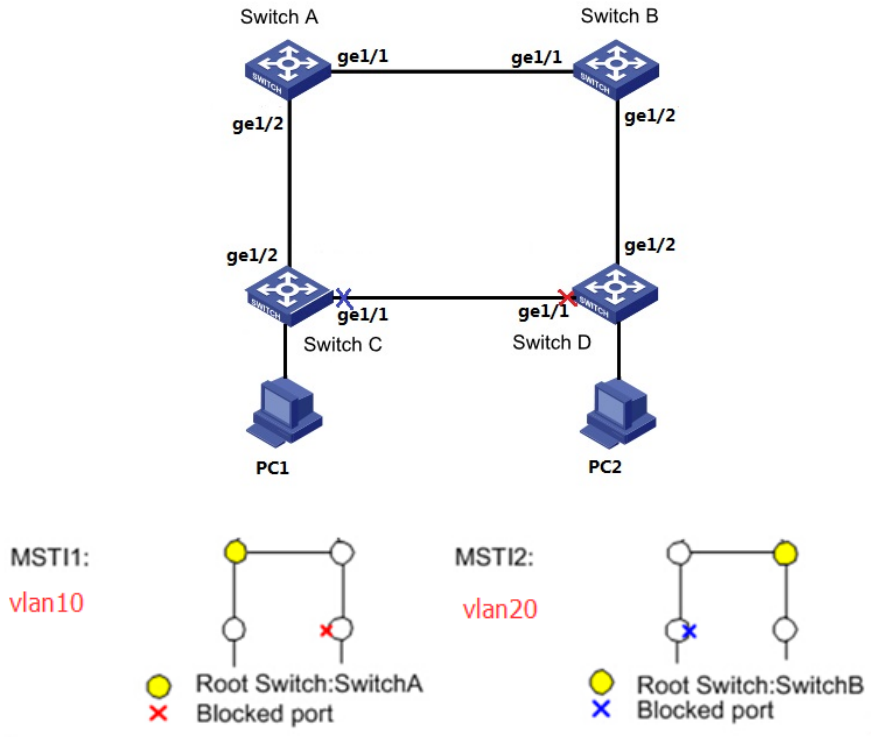
구성 항목	설명
MSTI	왼쪽 상단의 드롭 다운 상자를 통해 구성 할 인스턴스를 선택합니다.
Port	사용자가 구성 할 포트 선택.
Path Cost	인터페이스의 경로 비용 값을 입력하십시오. **0** 에서 **200,000,000** 범위의 값으로 **IEEE 802.1t** 표준을 사용하십시오
Priority	더 작은 값이 더 높은 우선 순위를 나타내는 포트 우선 순위를 선택하십시오. 인터페이스 우선 순위는 지정된 **MSTI** 의 인터페이스 역할에

	영향을줍니다. 다른 **MSTI** 에서 사용자는 동일한 인터페이스에 대한 우선 순위를 구성 할 수 있습니다. 결과적으로 서로 다른 **VLAN** 의 흐름이 물리적 링크를 따라 전달되어 **VLAN** 로드 공유를 달성 할 수 있습니다. 설명 : **MSTP** 는 인터페이스 역할을 다시 계산하고 우선 순위가 변경되면 해당 상태를 마이그레이션합니다.
Port Role	**3** 가지 유형의 루트 포트, 즉 지정된 포트, 백업 포트 및 비활성화 된 포트.
Port State	폐기, 전달 및 사용 안함의 **3** 개 상태 포함
Mode	현재 **STP** 모드
Type	인스턴스의 포트 유형에는 경계 및 내부 포트가 포함됩니다

2. 해당 구성 항목을 입력합니다.
3. “Apply” 하고 완료합니다.

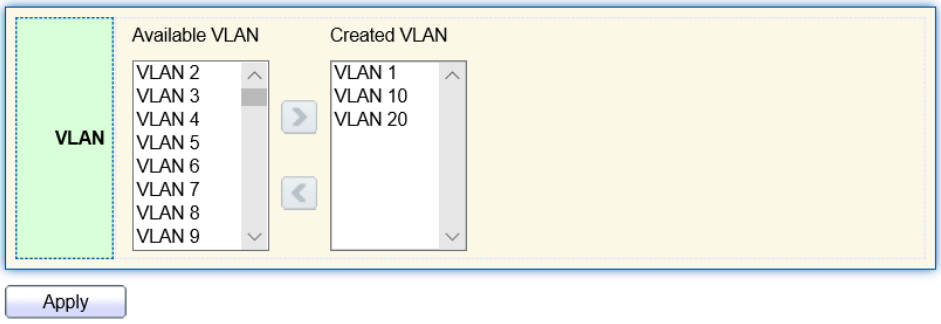
MST 기능 구성의 예시:

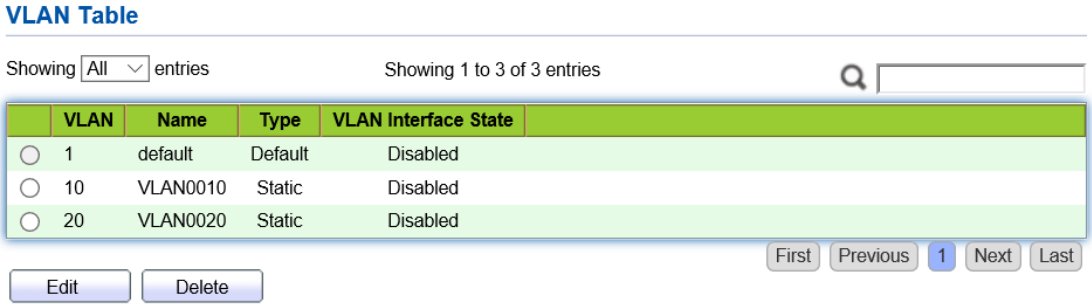
스위치 **A, B, C, D** 는 모두 **VLAN10** 및 **20** 의 부하를 공유하는 인스턴스를 도입하는 **MSTP** 를 실행합니다. **MSTP** 는 **VLAN** 매핑 테이블을 설정하여 **VLAN** 을 스패닝 트리 인스턴스와 연결하고 인스턴스 **1** 의 **VLAN10** 과 인스턴스 **2** 의 **VLAN20** 을 매핑 할 수 있습니다.



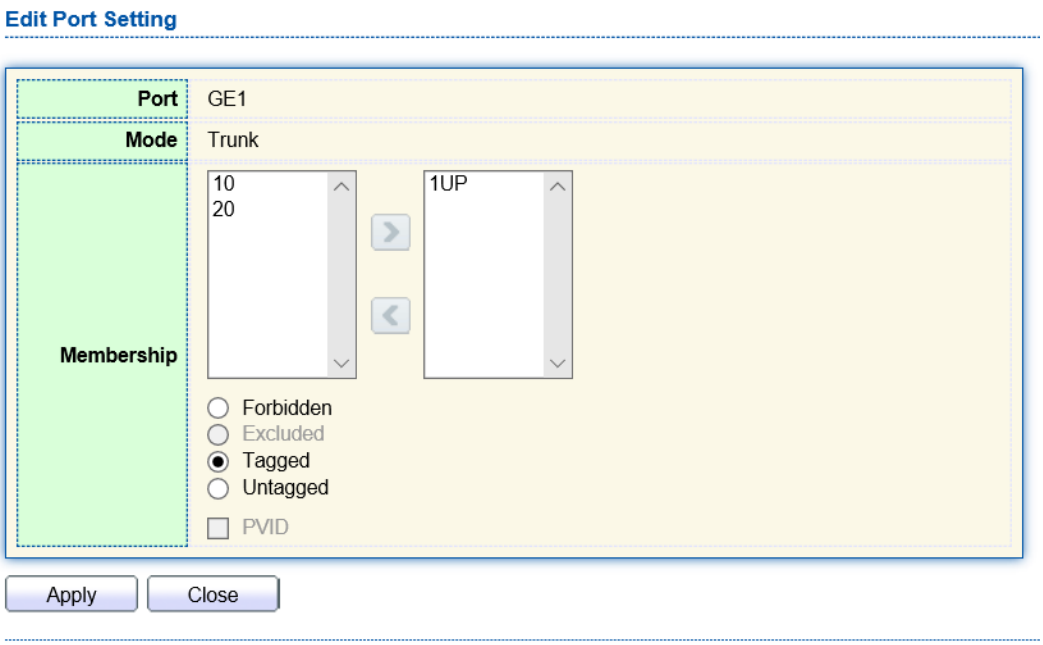
Instructions:

1. 스위치 **A, B, C, D** 는 링에있는 장치의 **L2** 전달 기능을 구성하기 위해 **VLAN10** 및 **20** 을 만듭니다. 탐색 트리에서 **"VLAN** 기능**> VLAN** 구성**> VLAN** 생성"을 클릭하고 해당 구성을 입력합니다. 다음과 같이 "Apply" 하고 완료합니다.

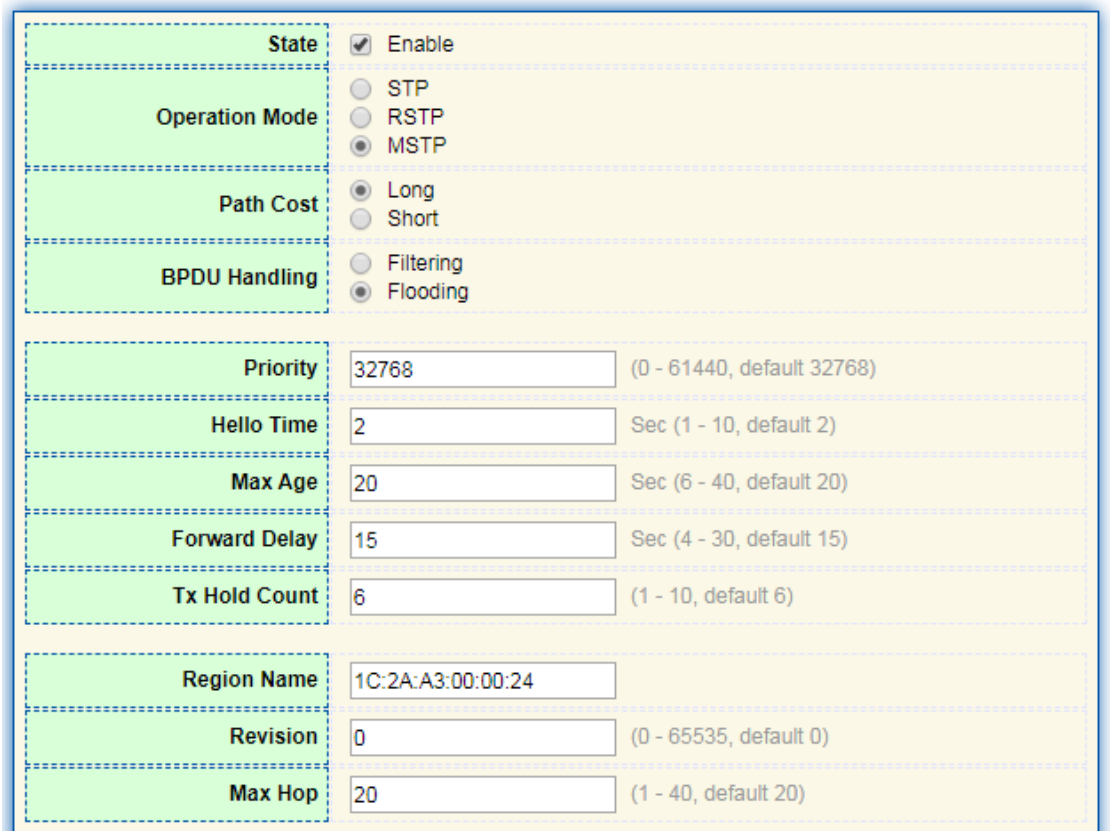




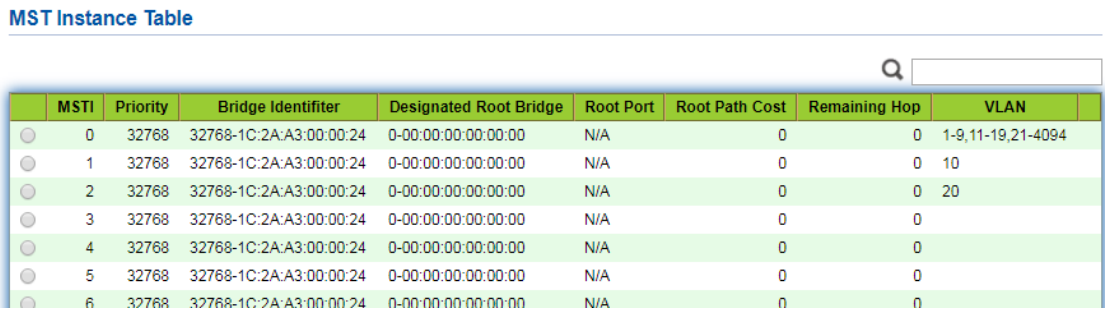
2. 탐색 트리에서 "VLAN > VLAN > Membership" 을 클릭하고 구성할 링 포트를 선택한 다음 VLAN10 및 20 을 오른쪽 상자로 이동시키고 "Tagged"로 표시합니다. "Apply" 하고 완료합니다:



3. 탐색 트리에서 “Spanning Tree > Property”을 클릭하고, 다음과 같이 MSTP 모드를 선택합니다:



4. 인스턴스 **MSTI1** 과 **MSTI2** 간의 **VLAN** 매핑을 구성합니다 “Spanning Tree > MST Instance”을 클릭하여 해당 매개 변수를 입력하고, “Add”를 클릭하여 설정을 마칩니다:



Note:

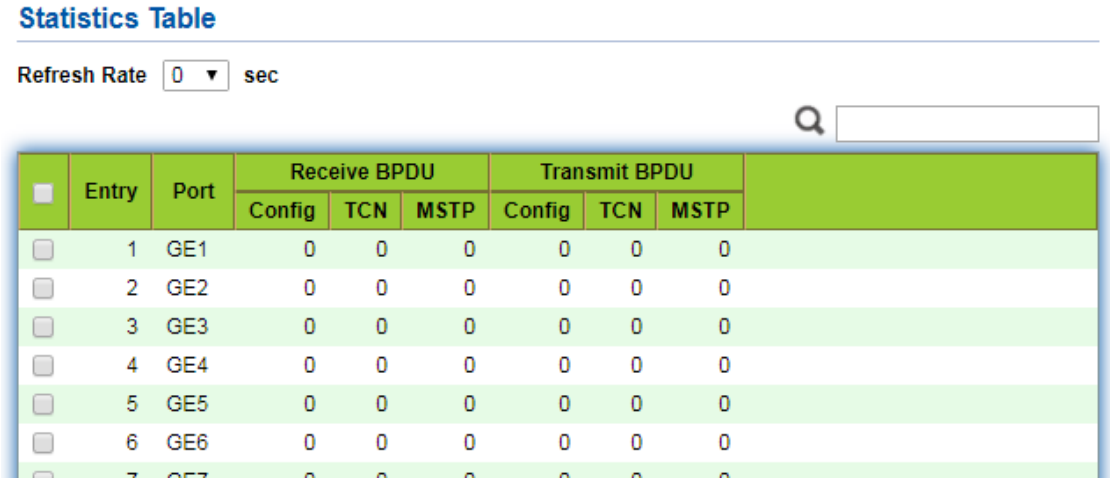
- 스위치 **A**를 구성하기 전에 **MSTI1**의 우선 순위를 **0**으로, **MSTI2**를 **4,096**으로 설정하십시오.
- 스위치 **B**를 구성하기 전에 **MSTI1**의 우선 순위를 **4,096**으로, **MSTI2**를 **0**으로 설정하십시오.
- 우선 순위는 **4,096**의 배수 여야합니다.

5. 스위치 **B**는 도메인에서 **MSTI2**의 루트 브리지와 **MSTI1**의 백업 루트 브리지 역할을합니다.

6. 나무 모양(Tree-Shaped)의 네트워크는 루프를 제거합니다

9.5 Statistics

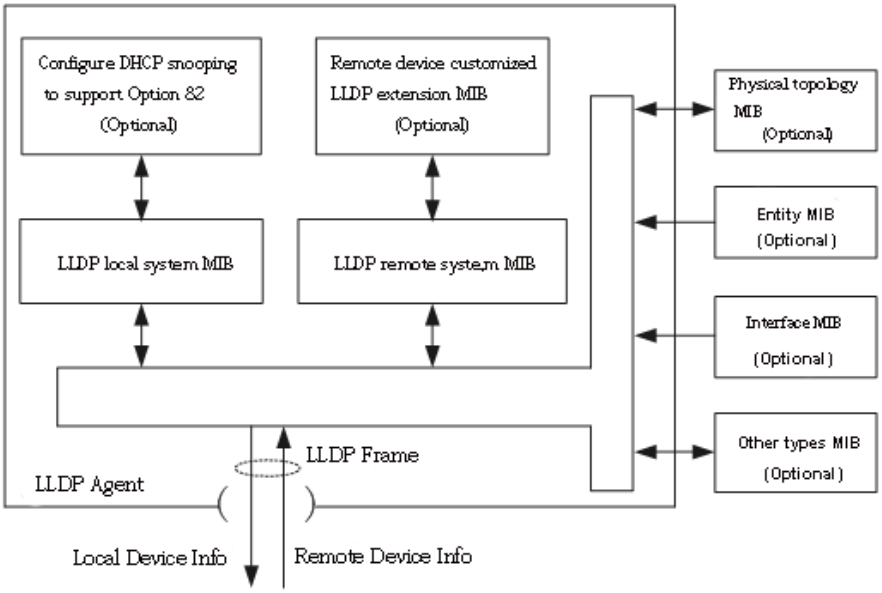
Instructions:
1. 탐색 트리에서 “Spanning Tree > Statistics”을 클릭합니다:



10 Discovery

LLDP (Link Layer Discovery Protocol)는 IEEE 802.1ab 에 정의되어 있습니다. 로컬 네트워크 장치의 관리 주소, 장치 및 인터페이스 식별과 같은 정보를 통합하여 인접 장치로 전송하는 표준 L2 검색 방법입니다. 정보를받은 후 NMS 쿼리 및 링크 통신 판단을위한 표준 MIB (Management Information Base) 형태로 저장합니다. 또한 정보를 통합하고 자체 원격 장치로 전송할 수 있습니다. 로컬 네트워크 장치에서받은 정보는 MIB 형식으로 보관됩니다. 다음은 작동 방식을 보여줍니다.

LLDP 블록 다이어그램



LLDP 는 다음을 기반으로 실현됩니다:

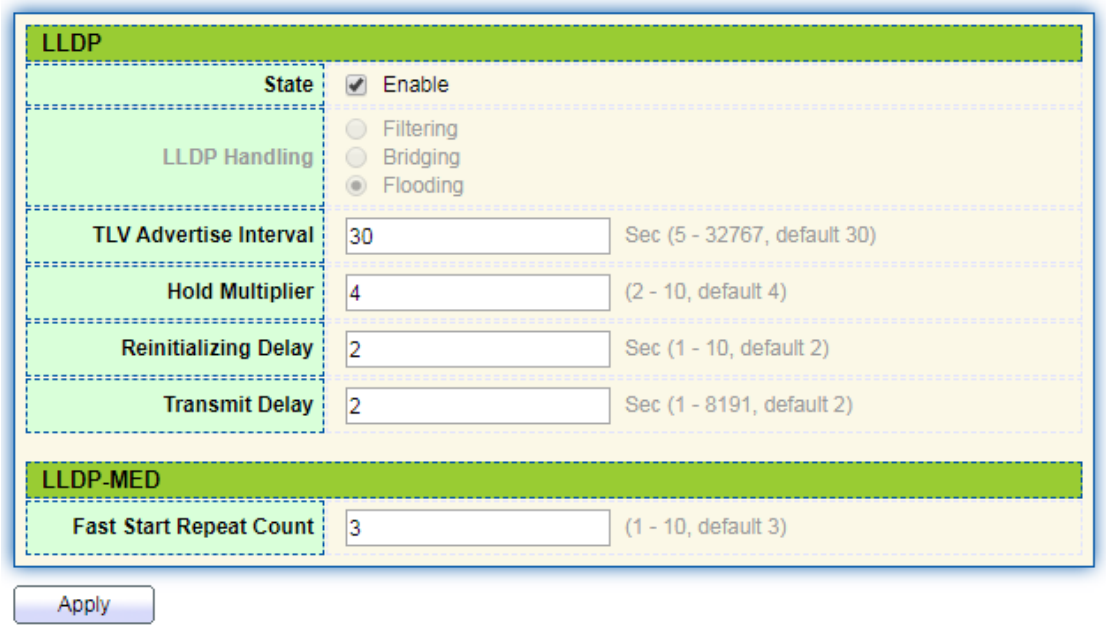
- **LLDP** 모듈은 물리적 토폴로지, 엔터티, 인터페이스 및 기타 유형의 **MIB** 와 **LLDP** 에이전트 간의 상호 작용을 통해 로컬 시스템 **MIB** 와 사용자 지정 확장 **MIB** 를 업데이트합니다.
- 로컬 네트워크 장치의 정보를 **LLDP** 프레임으로 캡슐화하여 원격 장치로 전송합니다.
- **LLDP** 원격 시스템 **MIB** 및 사용자 지정 확장 **MIB** 를 업데이트하기 위해 원격 장치에서 보낸 **LLDP** 프레임을 수신합니다.
- **LLDP** 에이전트의 송수신 기능을 통해 연결 인터페이스, **MAC** 주소 등 원격 장치의 정보를 마스터합니다.
- 로컬 시스템 **MIB** 는 장치 및 인터페이스 **ID**, 시스템 이름 및 설명, 인터페이스 설명, 네트워크 관리 주소 등을 포함한 로컬 장치 정보를 저장합니다.
- 원격 시스템 **MIB** 는 장치 및 인터페이스 **ID**, 시스템 이름 및 설명, 인터페이스 설명, 네트워크 관리 주소 등을 포함한 로컬 장치 정보를 저장합니다.

LLDP 를 기반으로 **LLDP-MED** 를 사용하면 다른 장치를 확장 할 수 있습니다. 네트워크 장치에서 확인한 정보는 장애 분석을 용이하게하고 관리 시스템을 통해 네트워크 토폴로지에 대한 정확한 이해를 심화시킵니다.

10.1 LLDP

Instructions:

1. 탐색 트리에서 “Discovery > LLDP > Property”를 클릭합니다.



구성 항목은 다음과 같습니다.

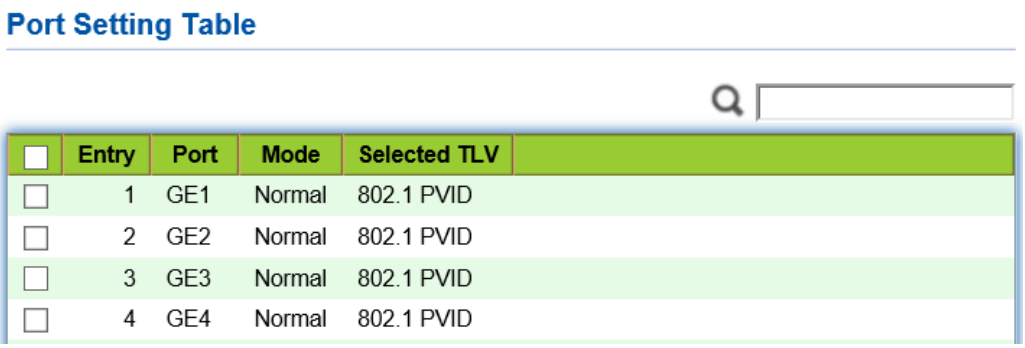
구성 항목	설명
State	**LLDP** 활성화 또는 비활성화
LLDP Handling	**LLDP** 메시지는 **LLDP** 를 비활성화 할 때 "필터링", "브리징"및 "플러딩"을 통해 처리됩니다.
TLV Advertise Interval	범위는 **5 ~ 32,768** 초입니다.(기본값 30)
Hold Multiplier	범위는 **2 ~ 10** 입니다.(기본값 4)
Reinitializing Delay	범위는 **1 ~ 10** 초입니다.(기본값 2)
Transmit Delay	범위는 **1 ~ 8,191** 초입니다.(기본값 2)
Fast Start Repeat Count	범위는 **1~10** 입니다.(기본값 3)

LLDPDU (LLDP Data Unit)로 캡슐화 된 이더넷 메시지는 **LLDP** 메시지로 인식됩니다. 각 **TLV** 는 지정된 정보와 함께 전달되는 **LLDPDU** 의 단위입니다.

2. 해당 구성 항목을 입력합니다
3. “Apply” 하고 완료합니다.

10.2 Port Setting

Instructions
1. 탐색 트리에서 “Discovery > LLDP > Port Setting” 을 클릭합니다.

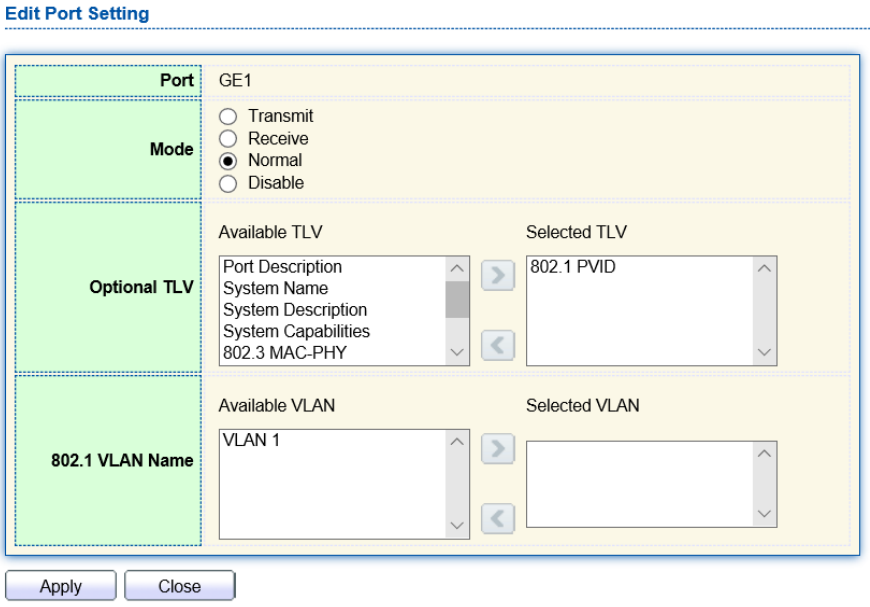


구성 항목은 다음과 같습니다.

구성 항목	설명
Port	포트 목록
Mode	LLDP 송수신 모드(기본값은 Normal) Transmit: LLDP 메시지만 전송합니다 Receive: LLDP 메시지만 수신합니다 Normal: **LLDP** 메시지 송수신 Disable: **LLDP** 메시지를 전송하거나 수신하지 않습니다.
Selected TLV	선택된 TLV 와 VLAN 정보

LLDP 는 4 가지 패턴으로 작동할 수 있습니다:
Transmit: LLDP 메시지를 송신만 합니다.
Receive: LLDP 메시지를 수신만 합니다.
Normal: LLDP 메시지를 송수신 합니다.
Disable: LLDP 메시지를 송신하거나 수신하지 않습니다.

2. “Edit”를 클릭해서 설정을 확인 및 수정하고, “Apply”하여 마칩니다.



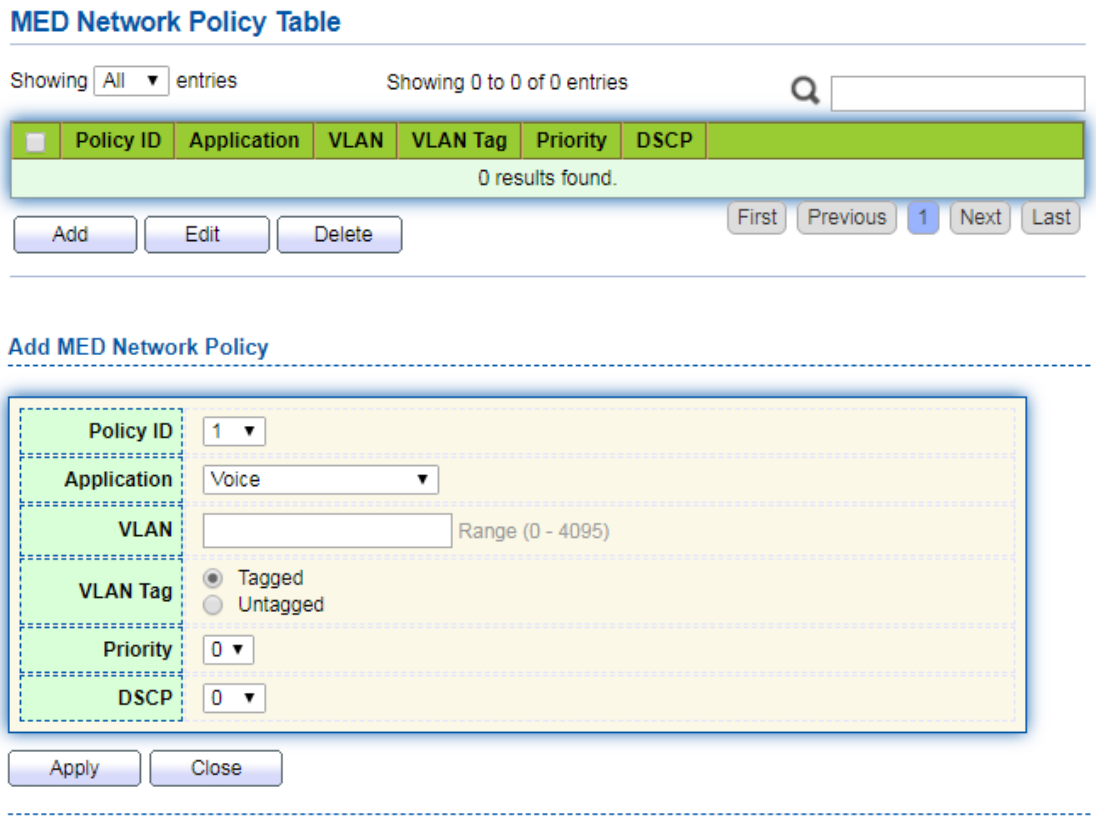
구성 항목은 다음과 같습니다.

구성 항목	설명
Port	포트 목록
Mode	LLDP 는 4 가지 패턴으로 작동할 수 있습니다: Transmit: LLDP 메시지를 송신만 합니다. Receive: LLDP 메시지를 수신만 합니다. Normal: LLDP 메시지를 송수신 합니다. Disable: LLDP 메시지를 송신하거나 수신하지 않습니다.
Optional TLV	**TLV** 및 **VLAN** 정보 선택
802.1 VLAN Name	**VLAN** 이름 선택

10.3 MED Network Policy

MED 는 IEEE 802.1ab 를 기반으로합니다. 스위치 및 무선 액세스 포인트와 같은 네트워크 장치에서 식별된 정보는 오류 분석에 도움이 될 수 있으며 관리 시스템이 네트워크 토폴로지를 정확하게 이해할 수 있도록 합니다.

Instructions
1. 탐색 트리에서 “Discovery > LLDP > MED Network Policy”를 클릭합니다.



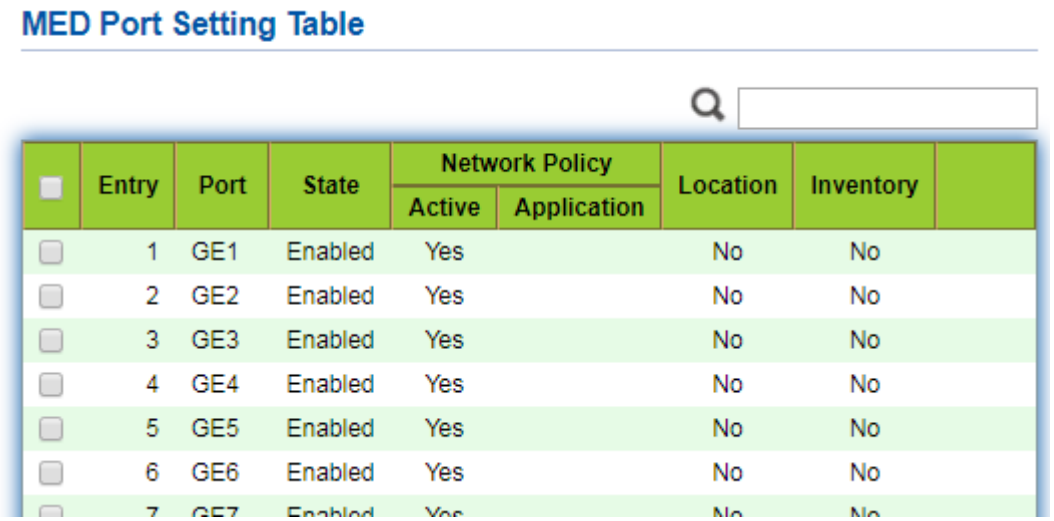
구성 항목은 다음과 같습니다.

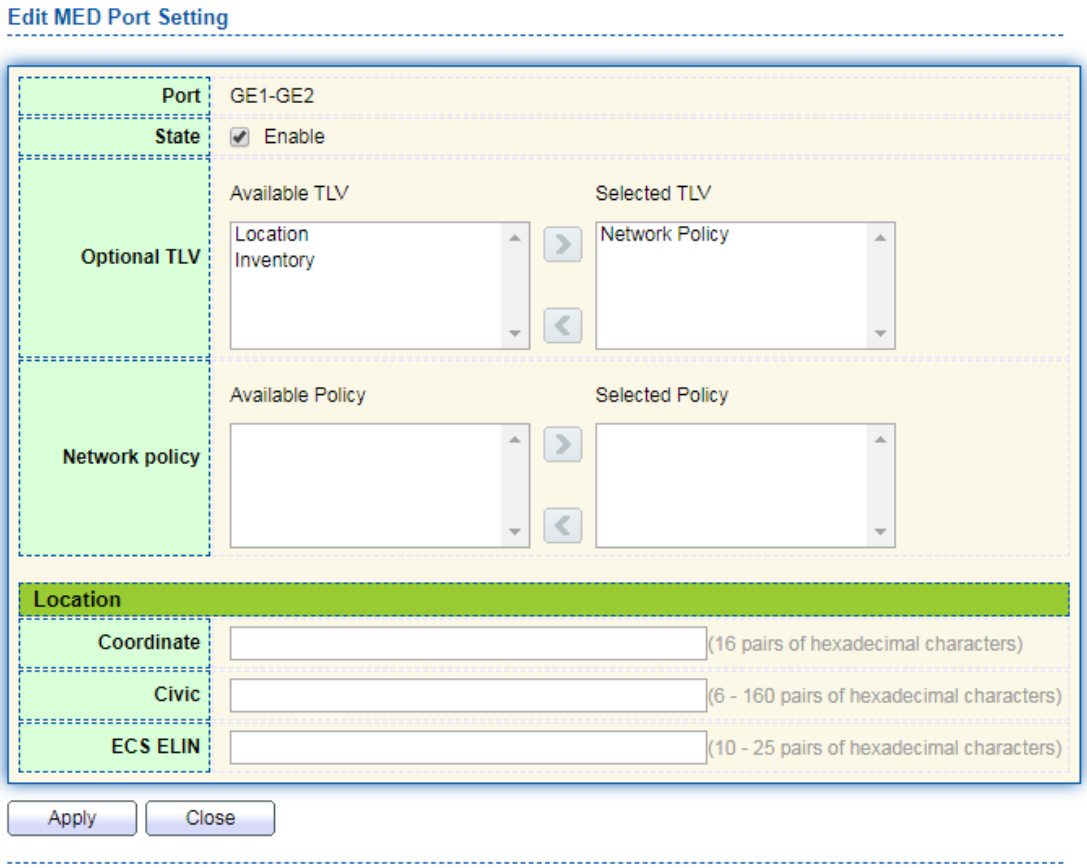
구성 항목	설명
Policy ID	Policy ID 번호
Application	network policy TLV 설정 및 적용
VLAN	VLAN 번호
VLAN Tag	VLAN 모드
Priority	CoS 서비스
DSCP	DSCP 서비스

10.4 MED Port Setting

Instructions

1. 탐색 트리에서 “Discovery > LLDP > MED Port Setting”을 클릭합니다.





구성 항목은 다음과 같습니다.

구성 항목	설명
Entry	MED port setting 의 시리얼 번호
Port	Port 목록
State	활성화 상태
Network Policy	network policy TLV 설정 및 적용
Location	location TLV 설정 및 적용

10.5 Packet View

Instructions

1. 탐색 트리에서 “Discovery > LLDP > Packet View”을 클릭합니다.

Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
○	1	GE1	38	1450	Not Overloading
○	2	GE2	38	1450	Not Overloading
○	3	GE3	38	1450	Not Overloading
○	4	GE4	38	1450	Not Overloading
○	5	GE5	38	1450	Not Overloading
○	6	GE6	38	1450	Not Overloading
○	7	GE7	38	1450	Not Overloading

10.6 Local Information

Device Summary 확인 방법:

1. 탐색 트리에서 “Discovery > LLDP > Local Information”을 클릭합니다.

Device Summary

Chassis ID Subtype	MAC address
Chassis ID	1C:2A:A3:00:00:24
System Name	Switch
System Description	HR-AFGM-2444S
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table 확인 방법:

2. 탐색 트리에서 “Discovery > LLDP > Local Information”을 클릭합니다.

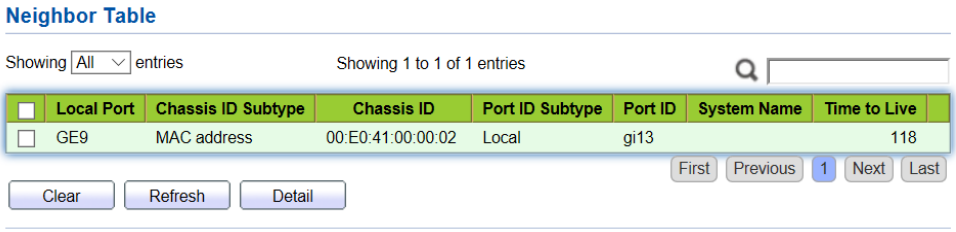
Port Status Table

	Entry	Port	LLDP State	LLDP-MED State
○	1	GE1	Normal	Enabled
○	2	GE2	Normal	Enabled
○	3	GE3	Normal	Enabled
○	4	GE4	Normal	Enabled
○	5	GE5	Normal	Enabled

10.7 Neighbor

LLDP neighbor 확인 방법:

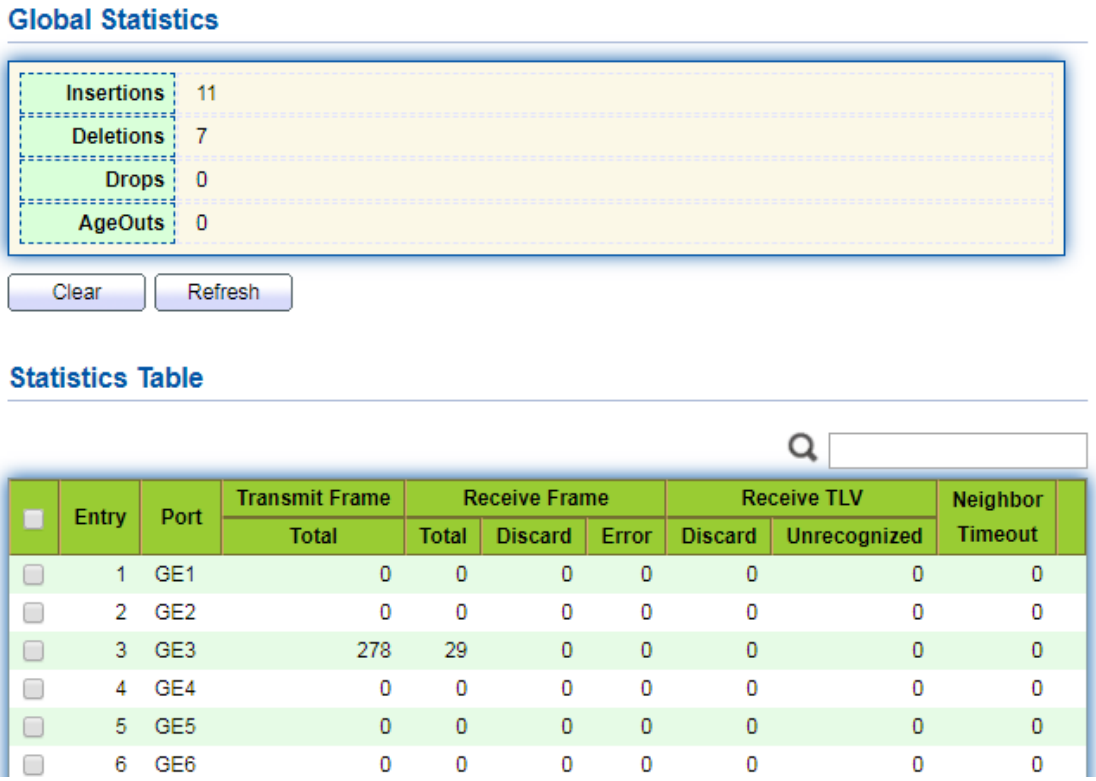
1. 탐색 트리에서 “Discovery > LLDP > Neighbor”을 클릭합니다.



10.8 Statistics

Instructions:

1. 탐색 트리에서 “Discovery > LLDP > Statistics”을 클릭합니다.



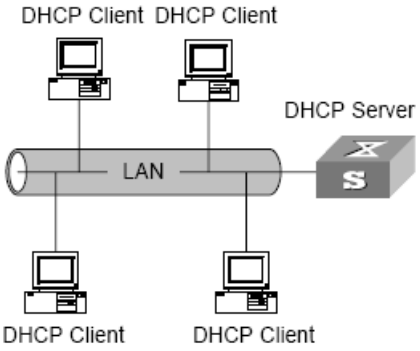
11 DHCP

DHCP Server 에 대하여.

네트워크 규모의 확장으로 인해 네트워크 구성이 점점 더 복잡해지고 있습니다. 컴퓨터 위치가 변경되고(예 : 휴대용 컴퓨터 또는 무선 네트워크) 컴퓨터 수가 할당 할 수 있는 IP 주소를 초과하는 경우가 발생할 수 있습니다.

DHCP(Dynamic Host Configuration Protocol)는 이러한 요구 사항을 충족하도록 개발되었습니다. DHCP 프로토콜은 클라이언트/서버 모드에서 작동합니다. DHCP 클라이언트는 DHCP 서버에 동적으로 구성 정보를 요청하고, DHCP 서버는 정책에 따라 해당 구성 정보를 반환합니다.

DHCP 의 일반적인 응용 프로그램에서는 일반적으로 다음 그림에 표시된 것처럼 DHCP 서버와 여러 클라이언트 (예 : PC 및 랩톱)가 포함됩니다.



<DHCP 의 구성 예시>

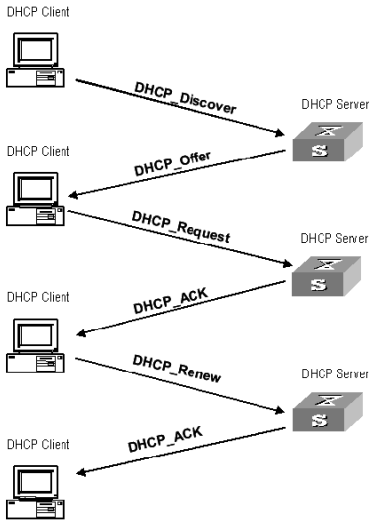
DHCP 의 IP 주소 할당

클라이언트의 다양한 요구에 따라 DHCP 는 세 가지 IP 주소 할당 방식을 제공합니다.

- 수동 주소 할당(Manual address assignment) : 관리자가 일부 특정 클라이언트 (예 : WWW 서버)에 대해 고정 IP 주소를 바인딩합니다. DHCP 를 통해 구성된 고정 IP 주소를 클라이언트로 보냅니다.
- 자동 주소 할당(Automatic address assignment) : DHCP 는 클라이언트에게 무제한 임대 기간으로 IP 주소를 할당합니다.
- 동적 주소 할당(Dynamic address assignment) : DHCP 는 유효 기간이있는 IP 주소를 클라이언트에 할당하며, 클라이언트는 서비스 수명이 만료 된 후 주소를 다시 신청해야합니다. 대부분의 클라이언트는 이 동적 주소 할당을받습니다.

10.2.2 Dynamic IP address 프로세스

DHCP 클라이언트와 DHCP 서버 간의 메시지 상호 작용 프로세스는 아래 그림과 같습니다.



<DHCP 상호 작용 프로세스>

동적 IP 주소를 얻기 위해 DHCP 클라이언트는 다른 단계에서 서버와 다른 정보를 상호 작용합니다. 일반적으로 다음과 같은 세 가지 모드가 있습니다.

(1) DHCP 클라이언트가 처음으로 네트워크에 로그인합니다.
DHCP 클라이언트가 처음 네트워크에 로그인 할 때 주로 4 단계를 통해 DHCP 서버와 연결을 설정합니다.

- DHCP 클라이언트가 처음 네트워크에 로그인 할 때 주로 4 단계를 통해 DHCP 서버와 연결을 설정합니다.
- 검색 단계(The discovery phase) : DHCP 클라이언트가 DHCP 서버를 찾는 단계입니다. 클라이언트는 브로드 캐스트 모드에서 DHCP 검색 메시지를 보내고 DHCP 서버 만 응답합니다.
- IP 주소 제공 단계(The stage of providing IP address) : 즉, DHCP 서버가 IP 주소를 제공하는 단계입니다. 클라이언트로부터 DHCP 검색 메시지를 수신 한 후 DHCP 서버는 IP 주소 풀에서 할당되지 않은 IP 주소를 선택하여 클라이언트에 할당하고 임대 된 IP 주소 및 기타 설정이 포함 된 DHCP 제안 메시지를 클라이언트에 보냅니다.
- 선택 단계(The selection stage) : DHCP 클라이언트가 IP 주소를 선택하는 단계입니다. 둘 이상의 DHCP 서버가 클라이언트에게 DHCP 제안 메시지를 보내는 경우 클라이언트는 처음 수신 된 DHCP 제안 메시지 만 수락 한 다음 각 DHCP 서버에 브로드 캐스트하여 DHCP 요청 메시지에 응답합니다.

이 정보에는 선택한 DHCP 서버에서 IP 주소를 요청하는 내용이 포함됩니다.

- 확인 단계(The confirmation stage) : DHCP 서버가 제공된 IP 주소를 확인하는 단계입니다. DHCP 서버가 DHCP 클라이언트가 응답 한 DHCP 요청 메시지를 수신하면 클라이언트가 제공 한 IP 주소 및 기타 설정이 포함된 dhcp-ack 확인 메시지를 보냅니다. 그렇지 않으면 클라이언트에 주소를 할당 할 수 없음을 나타내는 dhcp-nak 메시지를 반환합니다. 서버에서 반환 된 dhcp-ack 확인 메시지를받은 후 클라이언트는 주소 감지를 위해 브로드 캐스트 모드에서 ARP (대상 주소가 할당 된 주소)를 보냅니다. 지정된 시간 내에 응답이 수신되지 않으면 클라이언트는이 주소를 사용합니다..

(2) DHCP 클라이언트가 네트워크에 다시 로그온합니다.
DHCP 클라이언트가 네트워크에 다시 로그인하면 주로 다음 단계를 통해 DHCP 서버와 연결을 설정합니다.

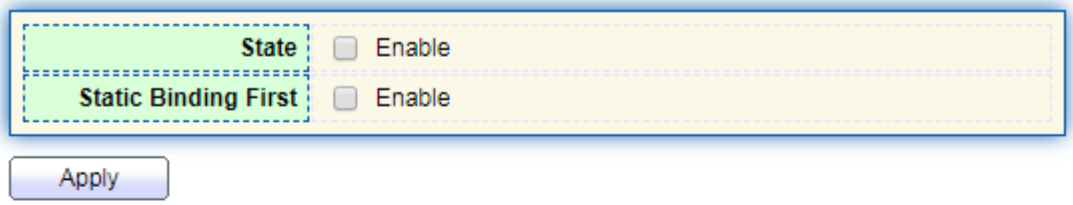
- DHCP 클라이언트가 처음 네트워크에 올바르게 로그인 한 후 다시 네트워크에 로그인 한 후 마지막에 할당 된 IP 주소가 포함된 DHCP 요청 메시지만 브로드 캐스트하면되고 DHCP 를 보낼 필요는 없습니다. 메시지를 다시 발견하십시오.
- DHCP 요청 메시지를받은 후 클라이언트가 요청한 주소가 할당되지 않은 경우 dhcp-ack 확인 메시지가 반환되어 원래 IP 주소를 계속 사용하도록 DHCP 클라이언트에 알립니다.
- IP 주소를 DHCP 클라이언트에 할당 할 수 없는 경우 (예 : 다른 클라이언트에 할당된 경우) DHCP 서버는 dhcp-nak 메시지를 반환합니다. 메시지를 받은 후 클라이언트는 새 IP 주소를 요청하기 위해 DHCP 검색 메시지를 다시 보냅니다.

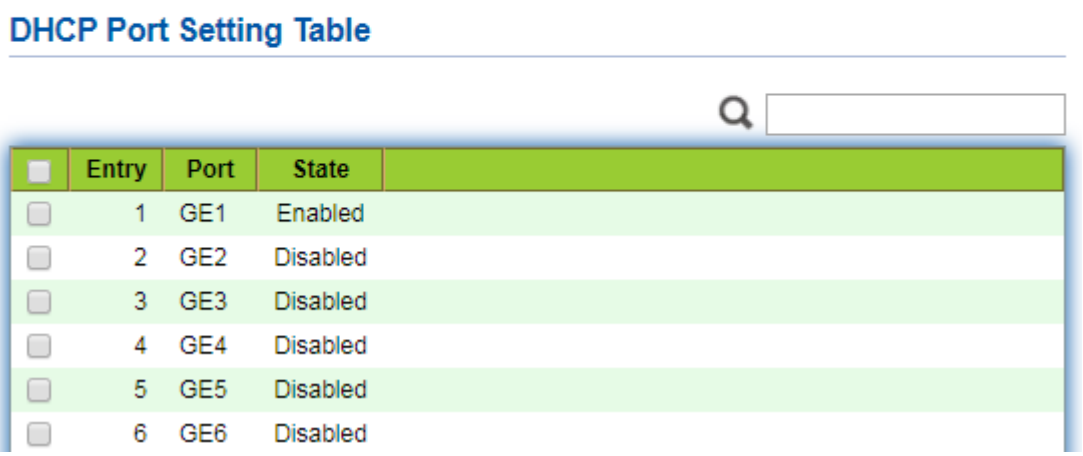
(3) DHCP 클라이언트는 IP 주소의 임대 유효 기간을 연장합니다.
DHCP 서버가 클라이언트에 할당 한 동적 IP 주소에는 일반적으로 특정 임대 기간이 있습니다. 만료 후 서버는 IP 주소를 다시 가져옵니다. DHCP 클라이언트가 주소를 계속 사용하려면 IP 임대를 업데이트해야합니다.
실제로 DHCP 클라이언트는 IP 주소 임대 기간이 절반에 도달하여 IP 임대 업데이트를 완료 할 때 기본적으로 DHCP 서버에 DHCP 요청 메시지를 보냅니다. IP 주소가 유효하면 DHCP 서버는 dhcp-ack 메시지에 응답하여 DHCP 클라이언트에 새 임대를 얻었음을 알립니다.

11.1 Property

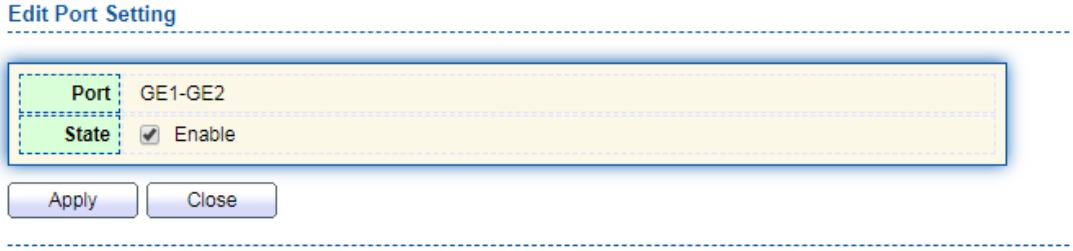
DHCP 글로벌 스태틱 바인딩 설정

Instructions:
1. 탐색 트리에서 “DHCP > Property”을 클릭합니다.





포트 DHCP 설정:
2. 탐색 트리에서 “DHCP > Property”을 클릭하고, 포트를 선택한 뒤 “Edit”하여 설정합니다.

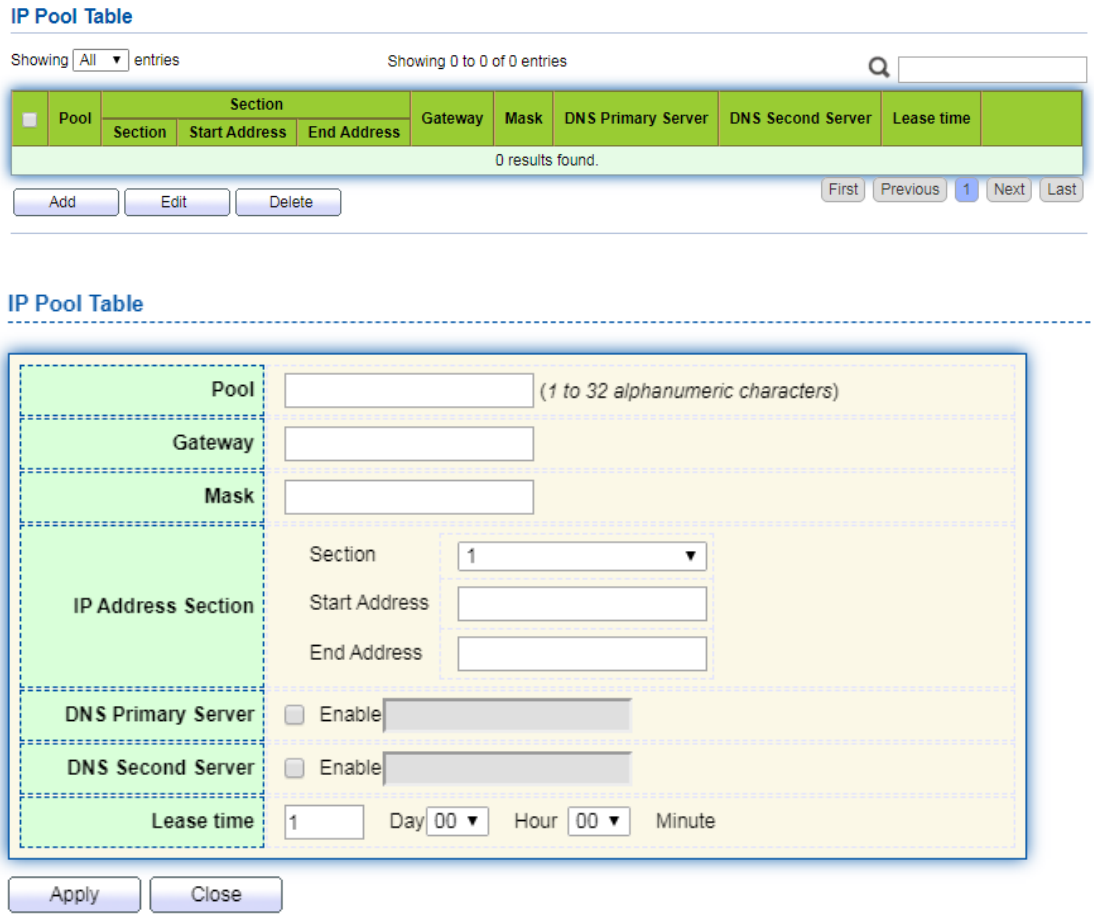


11.2 IP Pool Setting

DHCP IP pool 설정

Instructions:
1. 탐색 트리에서 “DHCP > IP Pool Setting”을 선택하고, “Add”를 클릭하여 ip

pool 을 추가합니다.



Note:

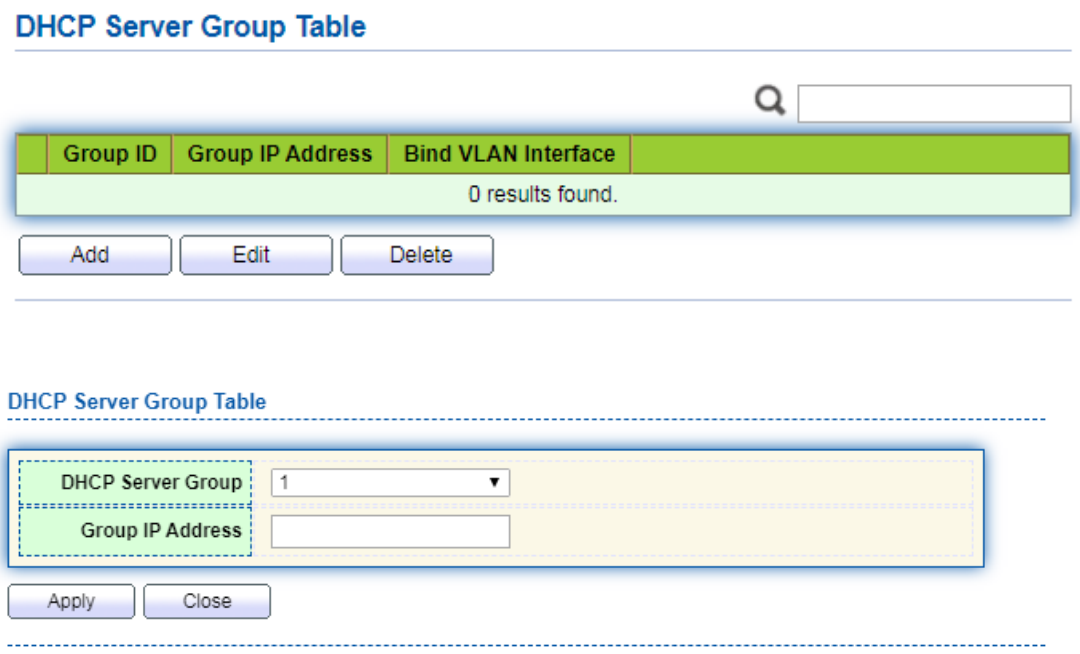
- 시작 주소와 끝 주소, 게이트웨이 주소를 포함하여 설정할 수 없습니다.

11.3 VLAN IF Address Group Setting

서버 그룹 설정

Instructions:

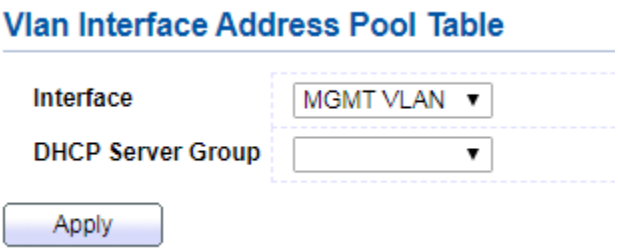
1. 탐색 트리에서 “DHCP > VLAN IF Address Group Setting”을 선택하고, DHCP Server Group Table에 들어가서, “Add” 를 클릭하여 서버 그룹을 설정합니다.



VLAN interface 와 server group 바인딩 설정

Instructions:

1. 탐색 트리에서 “DHCP > VLAN IF Address Group Setting”을 선택하고, VLAN Interface Address Pool Table 에 들어가서, 인터페이스와 서버 그룹을 선택한 다음, “Apply”하여 설정합니다.

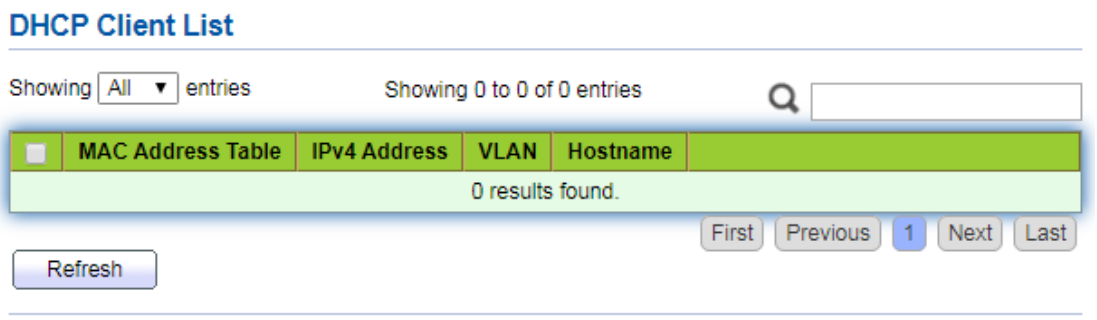


11.4 Client List

클라이언트 리스트 정보

Instructions:

1. 탐색 트리에서 “DHCP > Client List”를 선택하고, DHCP Client 목록에 들어갑니다.

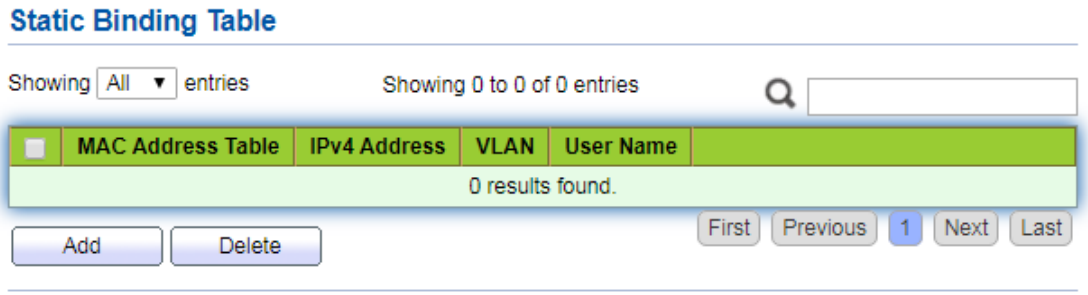


11.5 Client Static Binding Table

Static IP address 할당 설정

Instructions:

1. 탐색 트리에서 "DHCP > Client Static Binding Table"을 선택하여, Static Binding Table에 들어가서, "Add"를 클릭합니다.



Note:

- 정적 바인딩의 IP 구성은 IP 주소 할당 범위 내에 있어야합니다.

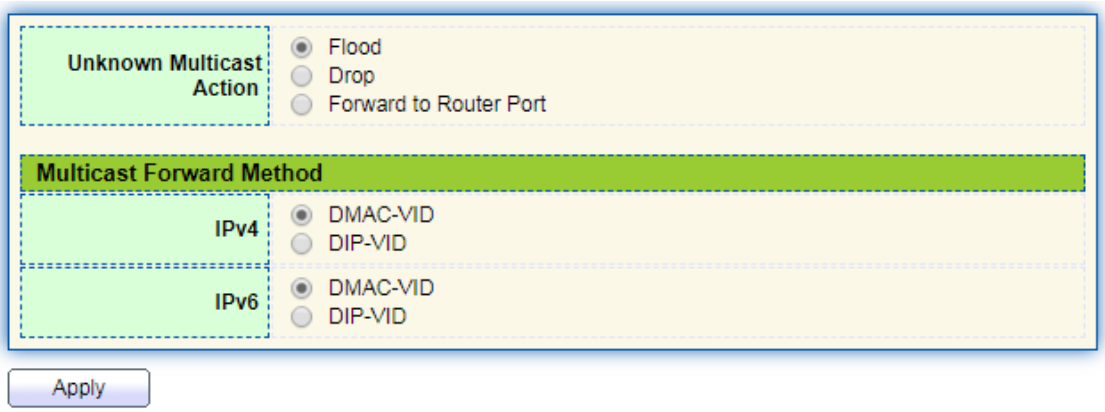
12 Multicast

12.1 General

12.1.1 Property

Instructions:

1. 탐색 트리에서 "Multicast > General > Property"을 선택합니다.

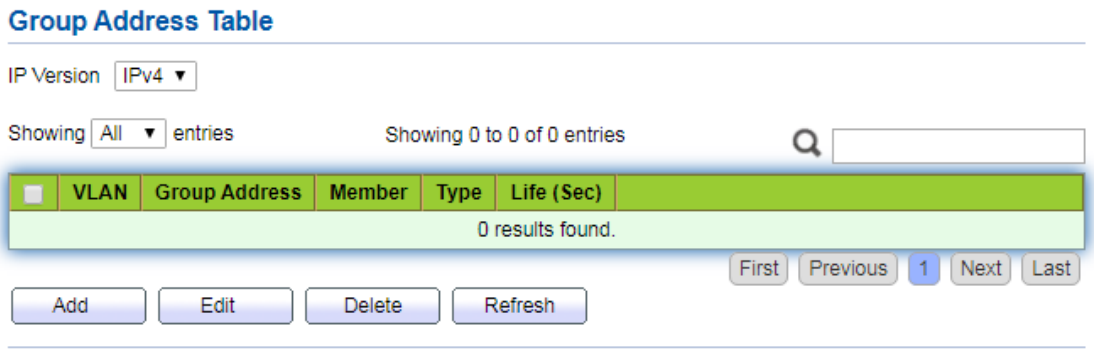


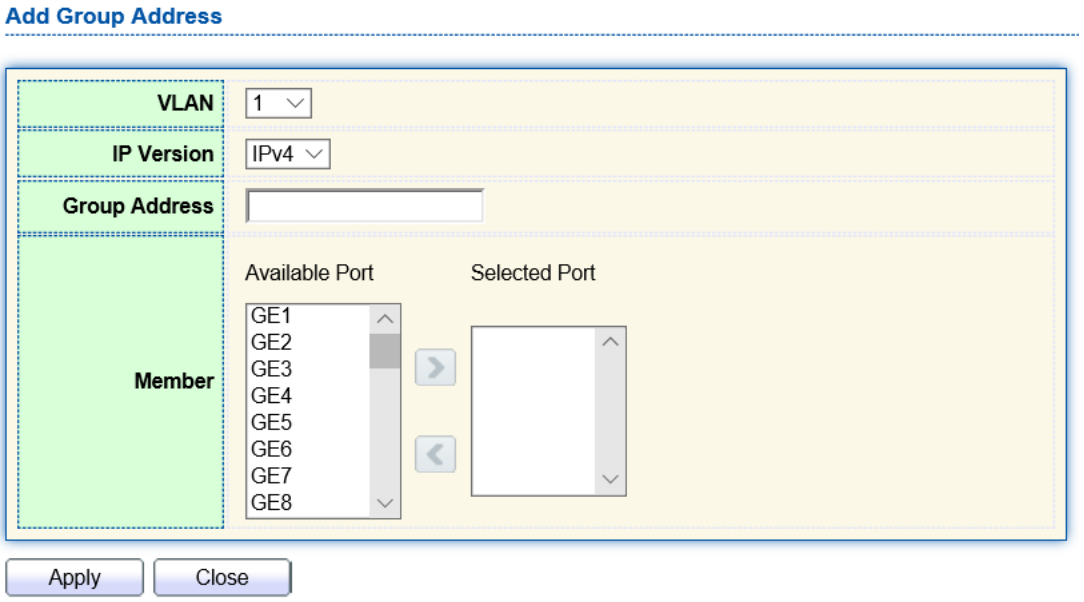
12.1.2 Group Address

멀티 캐스트의 이전 요청 모드에 따르면, 서로 다른 VLAN 에 있는 사용자가 동일한 멀티 캐스트 그룹을 요청할 때 멀티 캐스트 라우터는 데이터를 복사하여 수신자를 포함하는 각 VLAN 에 전달하여 많은 대역폭을 낭비합니다. IGMP 스누핑은 스위치 포트의 여러 사용자를 동일한 멀티 캐스트 VLAN 에 연결하여 멀티 캐스트 데이터를 수신함으로써 멀티 캐스트 VLAN 을 구성합니다. 이러한 방식으로 멀티 캐스트 플로우는 멀티 캐스트 VLAN 내에서만 전송될 수 있게 하므로 대역폭이 절약됩니다. 또한 멀티 캐스트 VLAN 이 사용자 VLAN 과 완전히 분리되어있어 보안 및 대역폭이 보장됩니다.

Instructions

1. 탐색 트리에서 “Multicast > Group Address”을 선택하고, 새 static multicast 아이템을 “Add”하거나, 기존 아이템을 “Edit” 합니다:

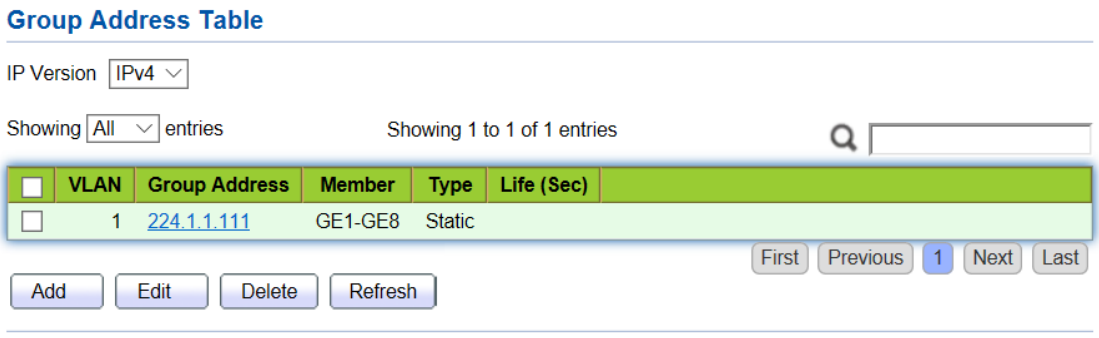




구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	멀티 캐스트 그룹이 속한 VLAN ID 입니다. 드롭 다운하여 기존 VLAN 을 선택합니다.
IP Version	v4 또는 v6 이 멀티 캐스트 IP 주소의 버전인지 여부
Multicast Address	multicast address 를 입력합니다.
Member	multicast member 를 입력합니다.

2. 해당 설정 항목을 입력합니다.
3. “Apply” 하여 완료합니다.

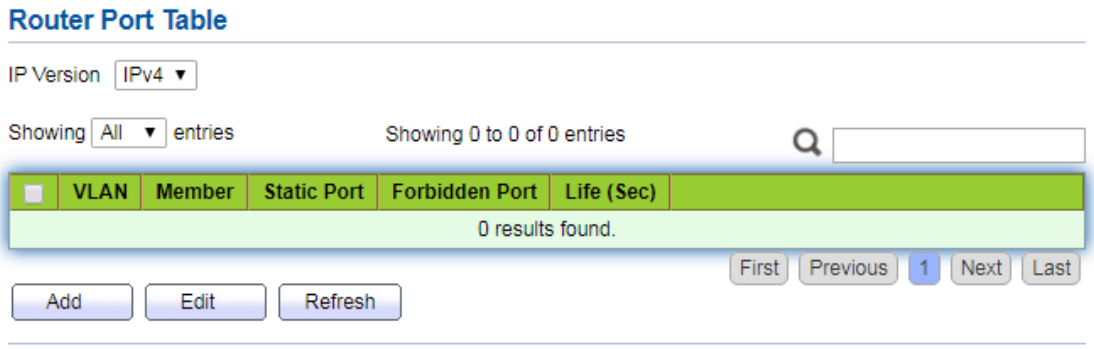


12.1.3 Router Port

multicast router port 설정 및 확인하기

Instructions:

1. 탐색 트리에서 “Multicast > General > Router Port”을 선택합니다.

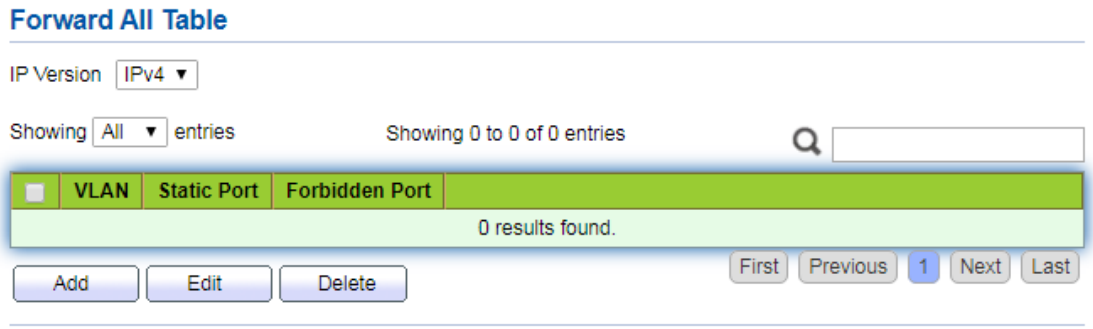


12.1.4 Forward All

multicast forward port 설정 및 확인하기

Instructions:

1. 탐색 트리에서 “Multicast > General > Forward All”을 선택합니다.

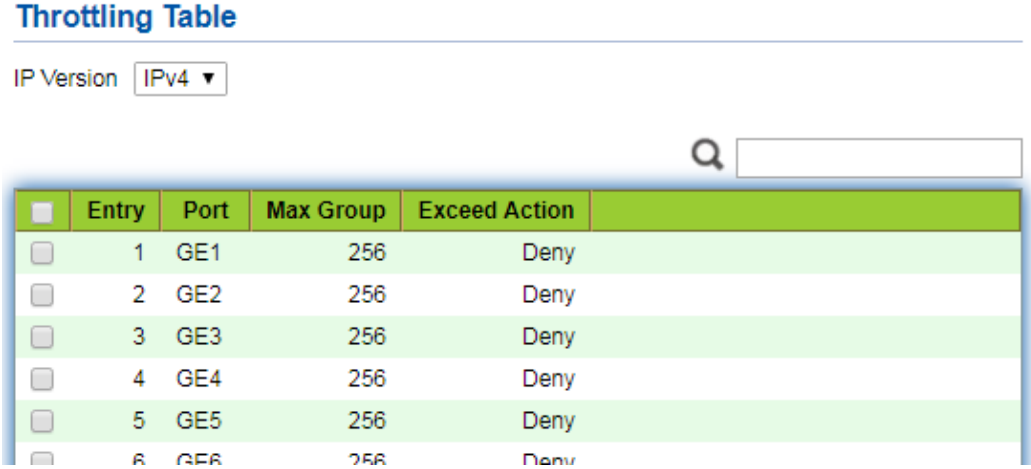


12.1.5 Throttling

port multicast group restrictions 설정 및 확인하기

Instructions:

1. 탐색 트리에서 “Multicast > General > Throttling”을 선택합니다.

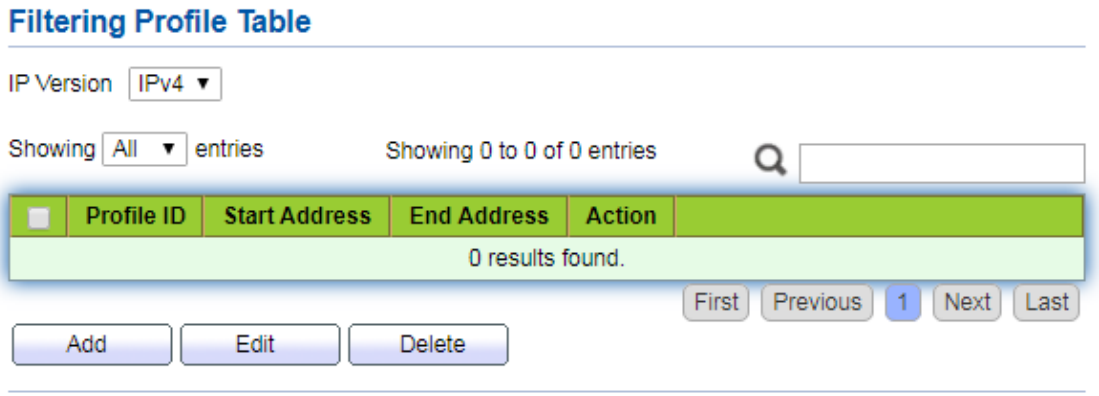


12.1.6 Filtering Profile

port multicast filtering profile 설정 및 확인하기

Instructions:

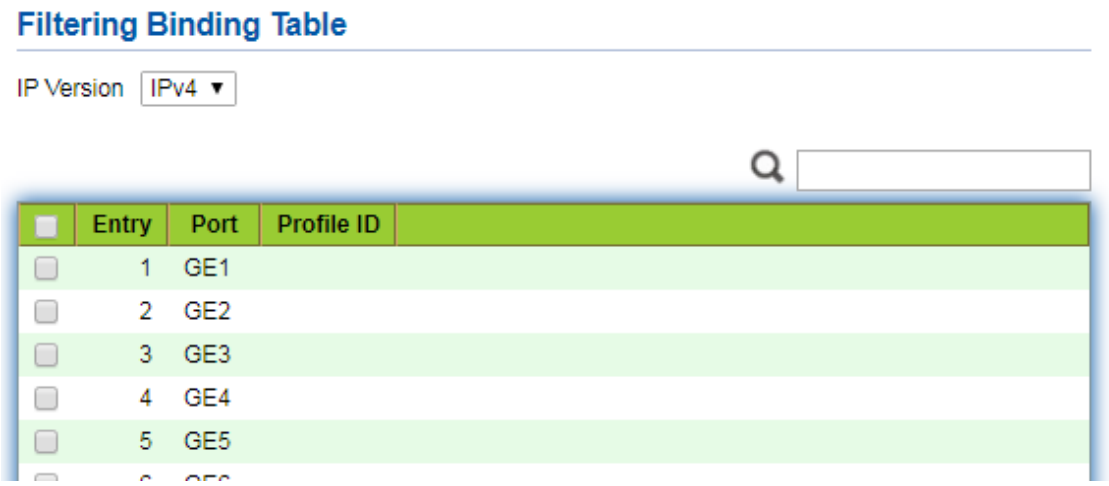
1. 탐색 트리에서 “Multicast > General > Filtering Profile”을 선택합니다.



multicast filtering profile and port binding relationship 설정 및 확인하기

Instructions:

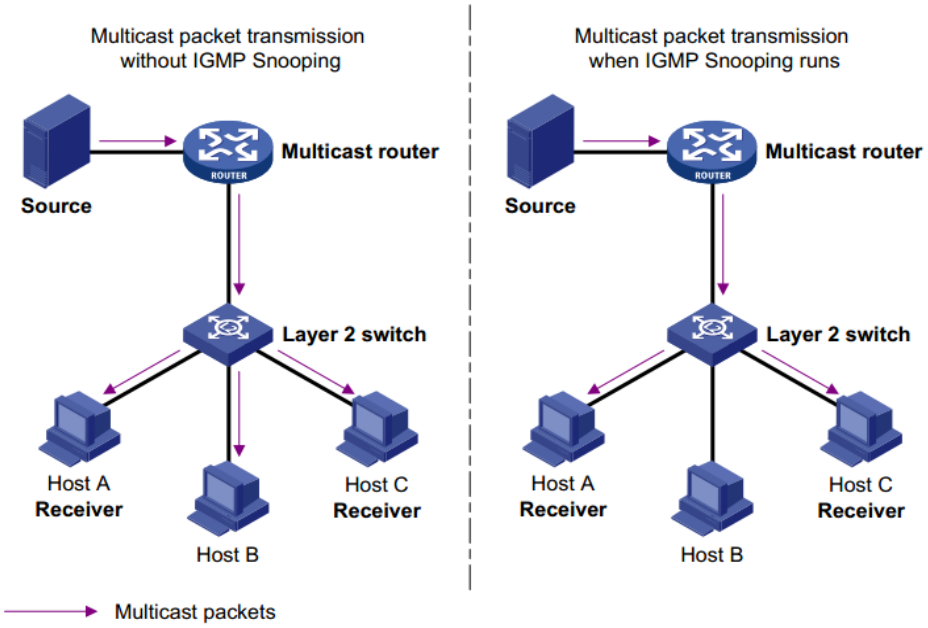
2. 탐색 트리에서 “Multicast > General > Filtering Binding”을 선택합니다.



12.2 IGMP Snooping

IGMP 스누핑 (인터넷 그룹 관리 프로토콜 스누핑)은 멀티 캐스트 그룹을 관리하고 제어하기위한 L2 장치의 제약 메커니즘입니다.
수신 된 IGMP 메시지를 분석하여 L2 장치는 포트와 MAC 멀티 캐스트 주소 간의 매핑을 설정하고 그에 따라 멀티 캐스트 데이터를 전달합니다.
아래와 같이 멀티 캐스트 데이터는 IGMP 스누핑없이 L2 에서 전송됩니다. IGMP 스누핑이 실행되면 알려진 멀티 캐스트 그룹 데이터가 지정된 수신기로 전송되고

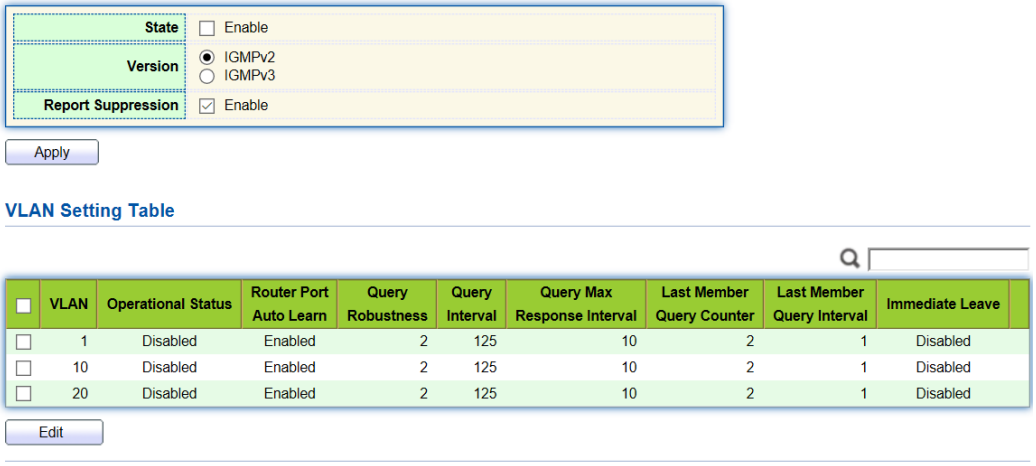
알 수없는 멀티 캐스트 데이터는 여전히 레이어 2 에 있습니다.

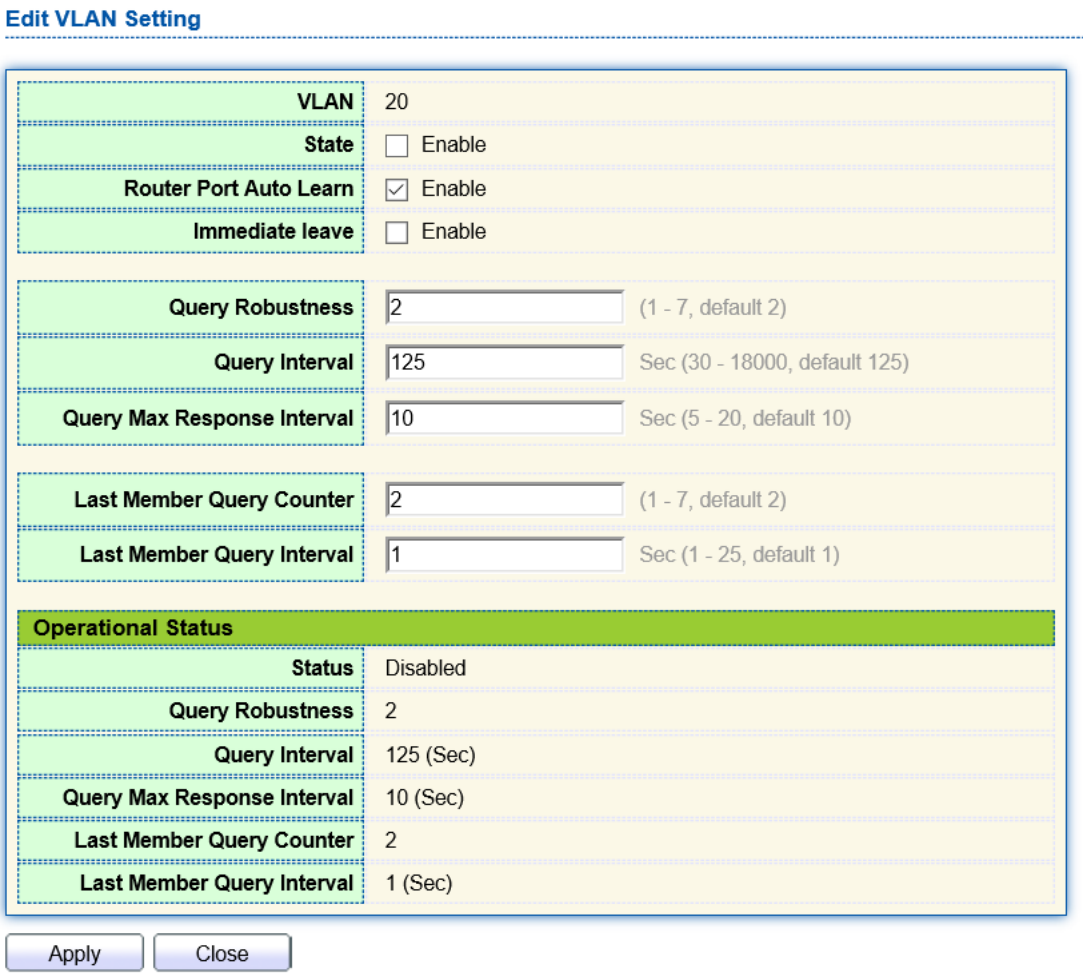


12.2.1 Property

IGMP 스누핑은 멀티 캐스트 라우터와 사용자 호스트 사이의 **L2** 스위치에 있으며 **IPv4** 네트워크를 배포하는 데 적용됩니다. 라우터와 호스트간에 전송되는 **IGMP / MLD** 메시지를 스누핑하고 멀티 캐스트 데이터에 대한 **L2** 포워딩 테이블을 설정하여 **L2** 네트워크에서 멀티 캐스트 데이터 포워딩을 관리 및 제어하도록 **VLAN** 에 구성됩니다.
글로벌 **IGMP** 스누핑 기능은 기본적으로 비활성화되어 있으므로 활성화해야합니다.

Instructions:
1. 탐색 트리에서 “Multicast > IGMP Snooping > Property”을 선택하고, 생성 된 **VLAN** 정보에서 구성할 **VLAN** 을 선택하고 다음과 같이 세부 정보를 “Edit”합니다:





구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	구성 할 **VLAN ID**
State	이 **VLAN** 에서 **IGMP** 스누핑 활성화 또는 비활성화
Router Port Auto Learn	경로 포트 자동 학습 활성화 또는 비활성화
Immediate leave	Multicast members 의 Immediate leave 활성화 또는 비활성화
Query Robustness	Robustness Variable 을 사용하여 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다.
Query Interval	메시지 쿼리 간격
Query Max Response Interval	쿼리 메시지의 시간 초과 **(**최대 응답 시간 초과**)**
Last Member Query Counter	지정된 그룹에 대한 최대 쿼리 수
Last Member Query	지정된 그룹에 대한 메시지 쿼리 간격

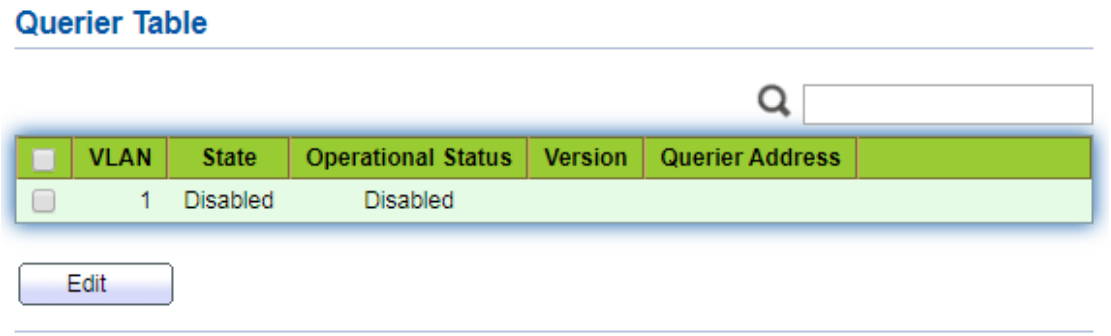
Interval	

2. 해당 설정 항목을 입력합니다.
3. “Apply”하여 설정을 마칩니다.

12.2.2 Querier

IGMP snooping Querier 설정 및 확인하기

Instructions:
1. 탐색 트리에서 “Multicast > IGMP Snooping > Querier”을 선택합니다.



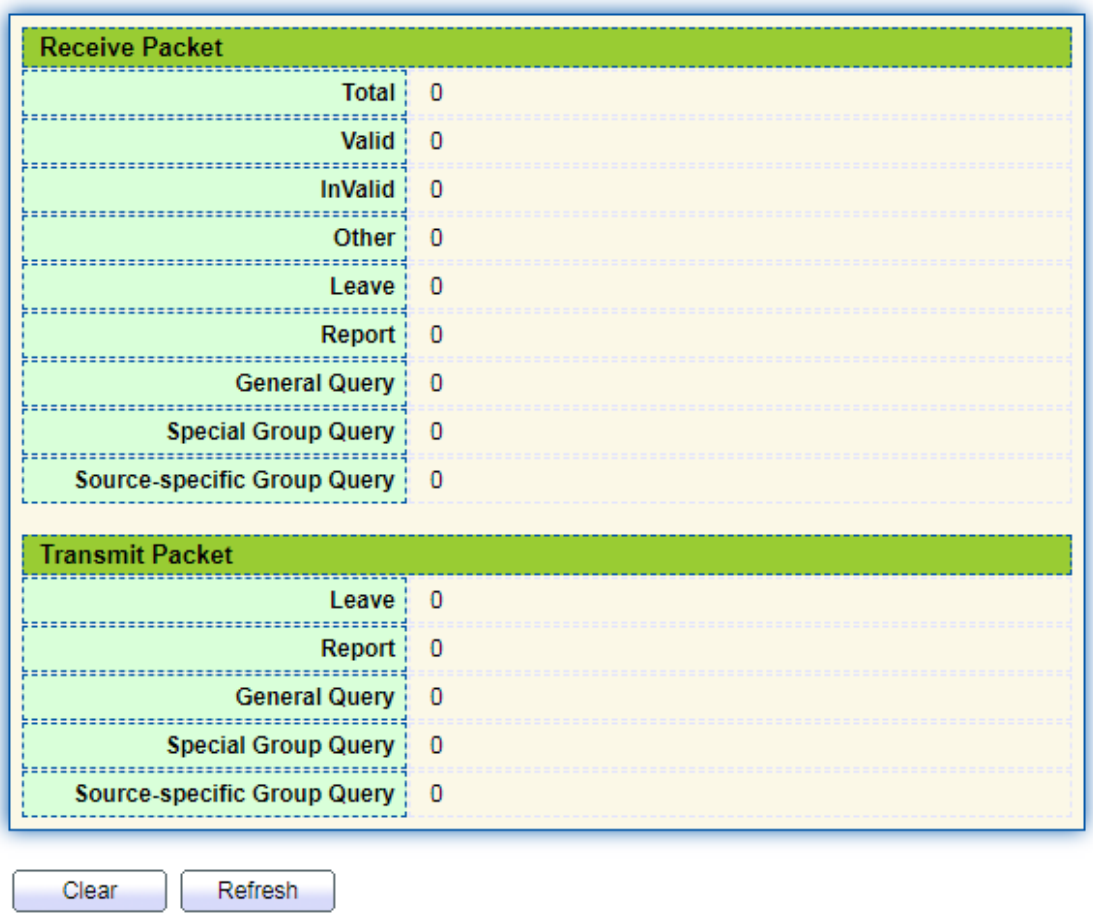
구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	Multicast VLAN
State	IGMP snooping querier를 활성화 또는 비활성화합니다.
Operational Status	IGMP snooping querier 동작 상태
Version	Querier의 버전
Querier Address	Querier의 Multicast address

12.2.3 Statistics

IGMP snooping statistics 설정 및 확인하기

Instructions:
1. 탐색 트리에서 “Multicast > IGMP Snooping > statistics”을 선택합니다.

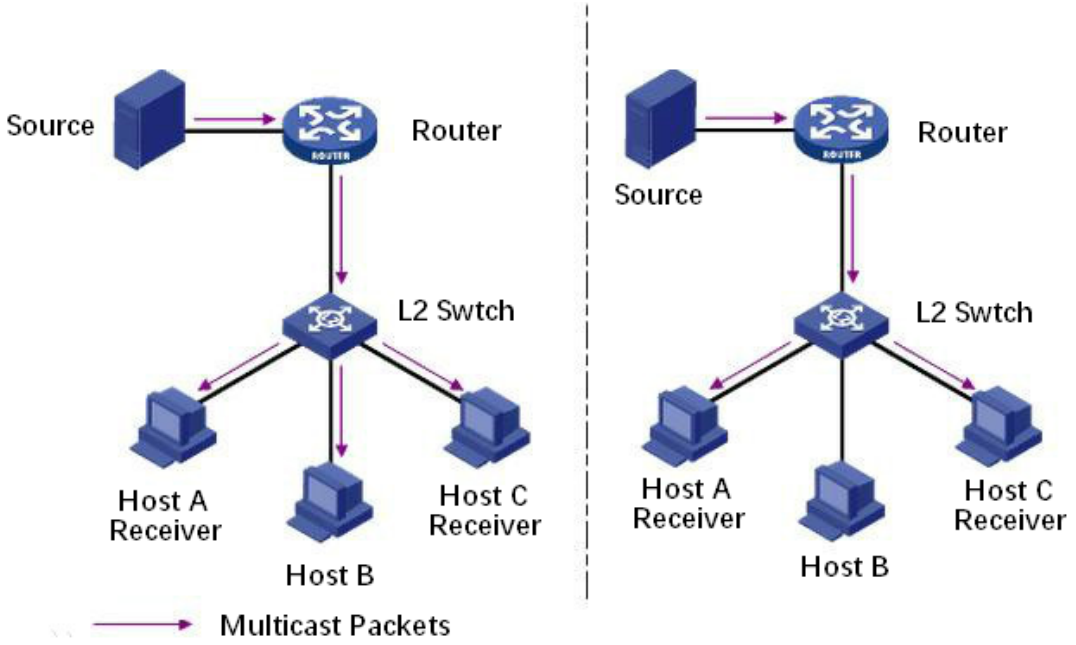


12.3 MLD Snooping

MLD 스누핑은 multicast Listener Discovery snooping 의 약자입니다. 이는 IPv6 멀티 캐스트 그룹을 관리하고 제어하는 데 사용되는 Layer2 장치에서 실행되는 IPv6 멀티 캐스트 제약 메커니즘입니다.

MLD 스누핑을 실행하는 Layer2 장치는 수신된 MLD 메시지를 분석하여 포트와 MAC 멀티 캐스트 주소 간의 매핑 관계를 설정하고 매핑 관계에 따라 IPv6 멀티 캐스트 데이터를 전달합니다.

아래 그림에서 볼 수 있듯이 Layer2 장치가 MLD 스누핑을 실행하지 않으면 IPv6 멀티 캐스트 데이터 패킷이 Layer2 에서 브로드 캐스트됩니다. Layer2 장치가 MLD 스누핑을 실행할 때 알려진 IPv6 멀티 캐스트 그룹의 멀티 캐스트 데이터 패킷은 계층 2 에서 브로드 캐스트되지 않고 계층 2 의 지정된 수신기로 멀티 캐스트됩니다.



MLD 스누핑은 Layer2 멀티 캐스트를 통해 필요한 수신자에게만 정보를 전달할 수 있으므로 다음과 같은 이점을 얻을 수 있습니다.:

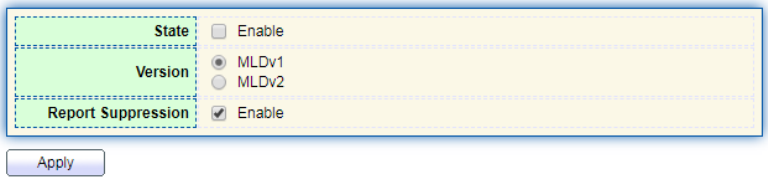
- Layer2 네트워크에서 브로드 캐스트 패킷을 줄이고 네트워크 대역폭을 절약합니다.;
- IPv6 멀티 캐스트 정보의 보안을 강화합니다.
- 각 호스트를 개별적으로 관리하는 것이 편리합니다.

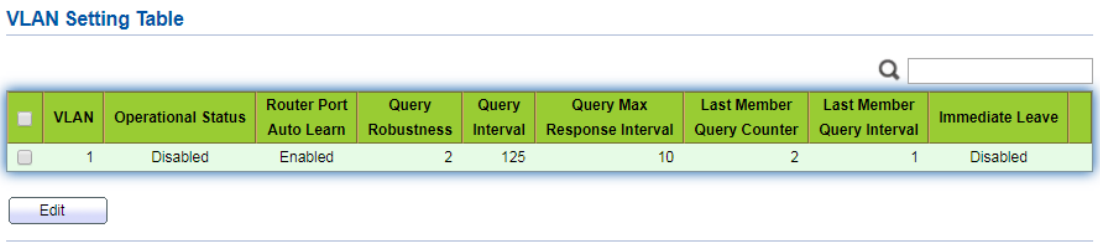
12.3.1 Property

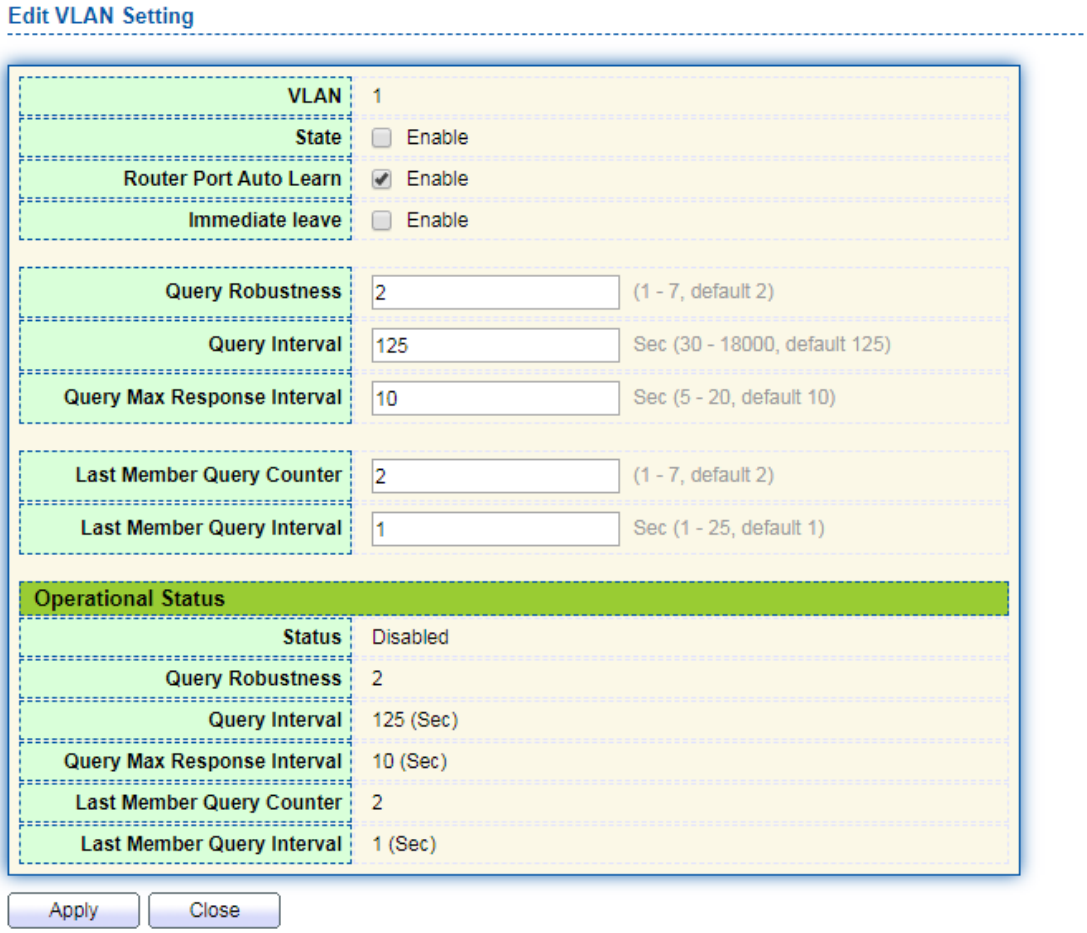
글로벌 MLD 스누핑 기능은 기본적으로 비활성화되어 있으므로 활성화해야합니다.

Instructions:

1. 탐색 트리에서 "Multicast > MLD Snooping > Property"을 선택하고, 생성 된 VLAN 정보에서 구성 할 VLAN 을 선택하고 다음과 같이 세부 정보를 "Edit" 합니다:







구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	VLAN ID
State	해당 VLAN 에서의 IGMP Snooping 활성화 또는 비활성화
Router Port Auto Learn	route port automatic learning 활성화 또는 비활성화
Immediate leave	Multicast members 의 immediate leave 설정
Query Robustness	Robustness Variable 을 사용하여 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다.
Query Interval	메시지 쿼리 간격
Query Max Response Interval	쿼리 메시지의 시간 초과 (최대 응답 시간 초과)
Last Member Query Counter	지정된 그룹에 대한 최대 쿼리 수
Last Member Query Interval	지정된 그룹에 대한 메시지 쿼리 간격

2. 해당 설정 항목을 입력합니다.
3. “Apply” 하여 설정을 마칩니다.

12.3.2 Statistics

MLD snooping statistics 설정 및 확인하기

Instructions:

1. 탐색 트리에서 “Multicast > MLD Snooping > statistics” 을 선택합니다.

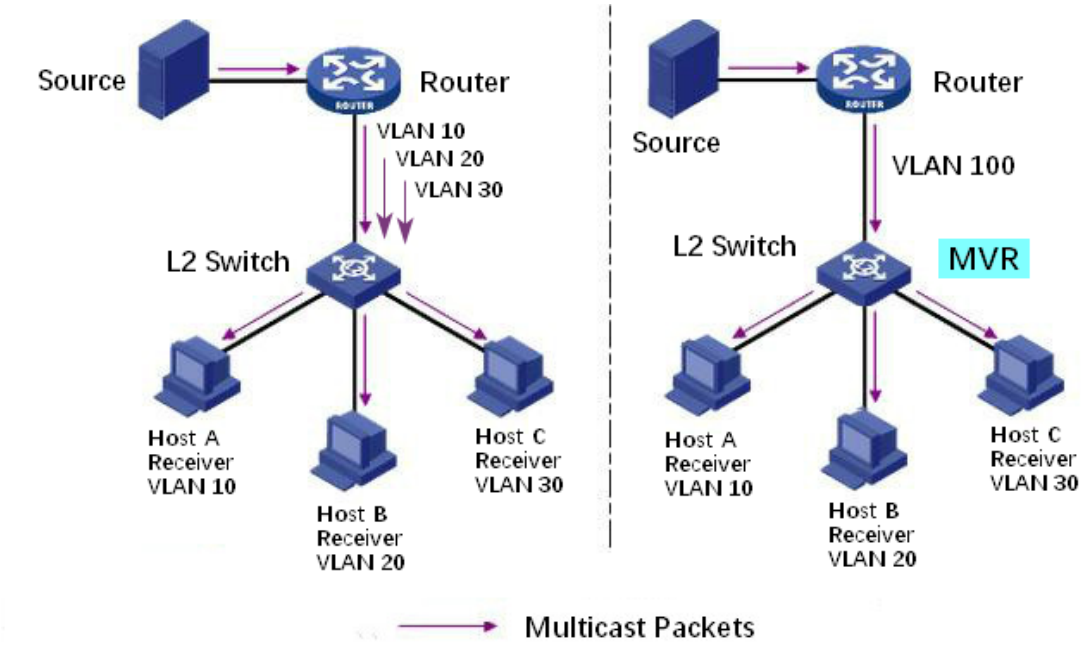


12.4 MVR

레이어 2 네트워크에서 VLAN 기반의 멀티 캐스트 트래픽 브로드 캐스트 문제를 해결하기 위해 IGMP 스누핑 프로토콜을 사용하여 수신기를 제어합니다. 즉, 수신기 만 정상적으로 멀티 캐스트 트래픽을 수신할 수 있습니다.

그러나 IGMP 스누핑은 동일한 멀티 캐스트 VLAN 의 트래픽 만 효과적으로 제어할 수 있지만 교차 VLAN 트래픽은 제어할 수 없습니다. 그 결과 서로 다른 VLAN 에서

동일한 멀티 캐스트의 다중 복제 효율성이 여전히 존재합니다. 크로스 VLAN 의 플러딩 문제를 해결하기 위해 아래 그림과 같이 멀티 캐스트 소스 트래픽의 전용 멀티 캐스트 VLAN 을 채택합니다.

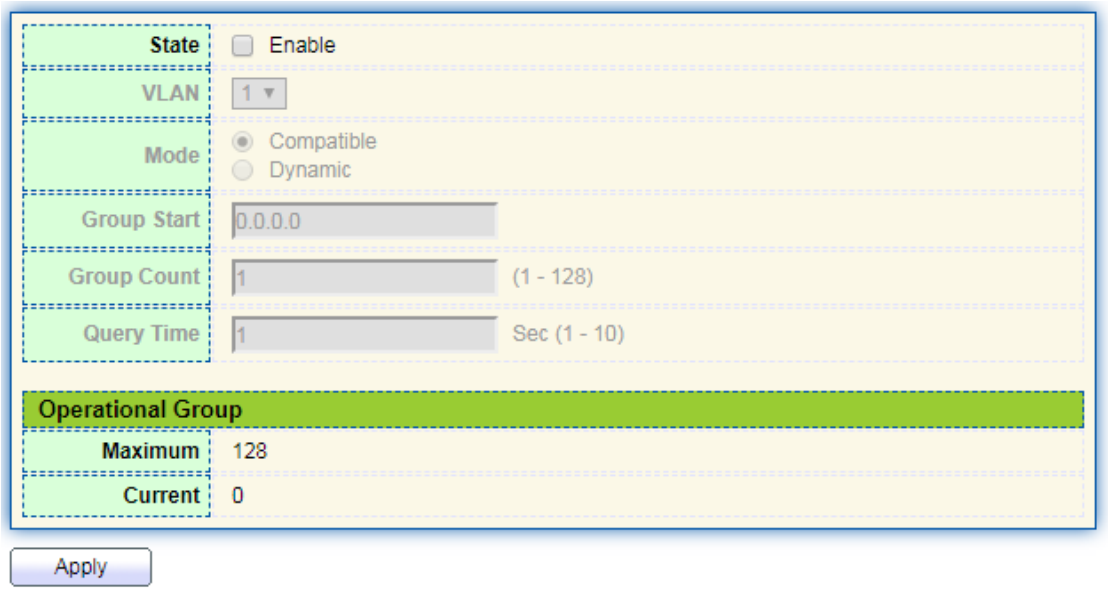


12.4.1 Property

글로벌 MVR 기능은 기본적으로 비활성화되어 있으므로 활성화해야합니다.

Instructions:

1. 탐색 트리에서 “Multicast > MVR > Property”을 클릭해서, MVR global configuration 에 들어갑니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
State	MVR 을 활성화 또는 비활성화 합니다.
VLAN	설정할 VLAN ID
Mode	Compatible: MVR 스위치의 CPU 는 일반적으로 라우터의 쿼리 메시지와 클라이언트의 조인 메시지를 전달하여 동적 학습의 멀티 캐스트 전달 테이블을 구성합니다. 그러나 CPU 는 결합 메시지를 라우터 포트로 전달하지 않으므로 상위 라우터는 다음 결합 메시지를 수신하지 못하여 라우터 데이터를 스위치로 정상적으로 전달할 수 없습니다. 이 모드에서는 라우터를 수동으로 구성해야합니다. 멀티 캐스트 전달 테이블은 데이터를 전환하기 위해 전달합니다. Dynamic: 동적 모드와 호환 모드의 유일한 차이점은 CPU 가 동적 모드에서 라우터 포트에 조인 메시지를 전달할 수 있으므로 상위 계층 라우터가 멀티 캐스트 전달 테이블을 동적으로 학습 할 수 있다는 것입니다. 데이터를 스위치로 전달하도록 라우터의 멀티 캐스트 전달 테이블을 수동으로 구성합니다.
Group Start	멀티 캐스트 그룹의 시작 주소
Group Count	멀티 캐스트 그룹 주소 수
Query Time	멀티 캐스트 그룹 쿼리 시간

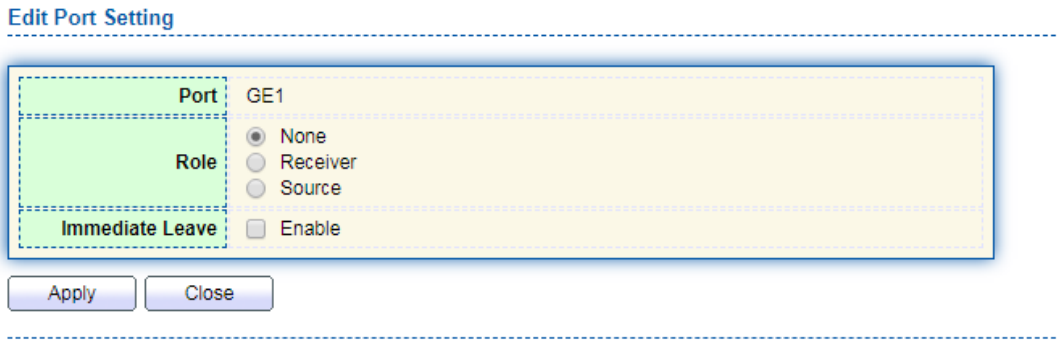
2. 해당 설정 항목을 입력합니다.
3. “Apply” 하여 설정을 마칩니다.

12.4.2 Port Setting

Instructions:

1. 탐색 트리에서 “Multicast > MVR > Port Setting” 을 선택하고, MVR port setting 인터페이스에 들어갑니다:





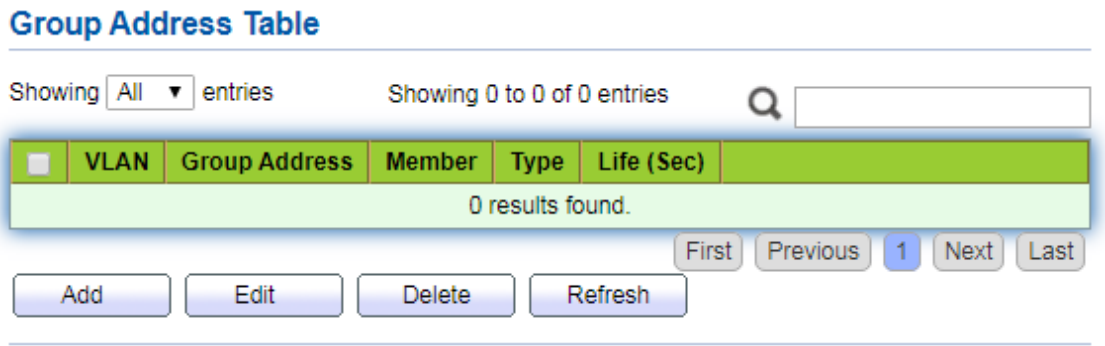
구성 항목은 다음과 같습니다.

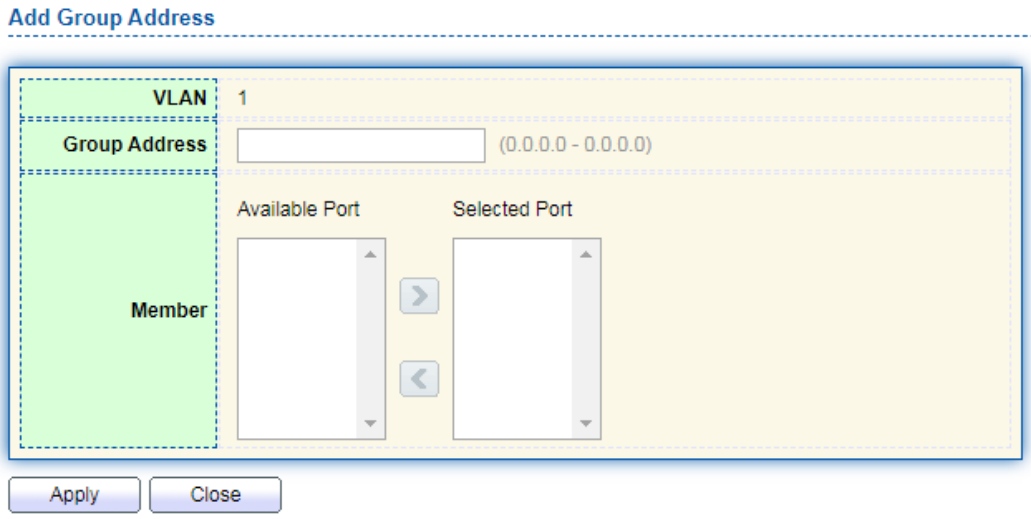
구성 항목	설명
Port	포트 목록
Role	포트 모드 Receiver: 멀티 캐스트 스트림을 수신하는 데 사용되는 멀티 캐스트 호스트가 연결된 스위치의 포트를 나타냅니다. Source: 소스 포트는 상위 계층 장비의 멀티 캐스트 흐름의 소스 포트, 즉 멀티 캐스트 소스 액세스 포트를 나타냅니다.
Immediate Leave	Immediate Leave 를 설정합니다.

12.4.3 Group Address

Instructions:

1. 탐색 트리에서 “Multicast > MVR > Group Address”를 선택하고, multicast group 정보를 확인합니다:





구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	VLAN ID
Group Address	multicast address 를 입력합니다.
Member	multicast member 를 추가합니다.

13 Routing

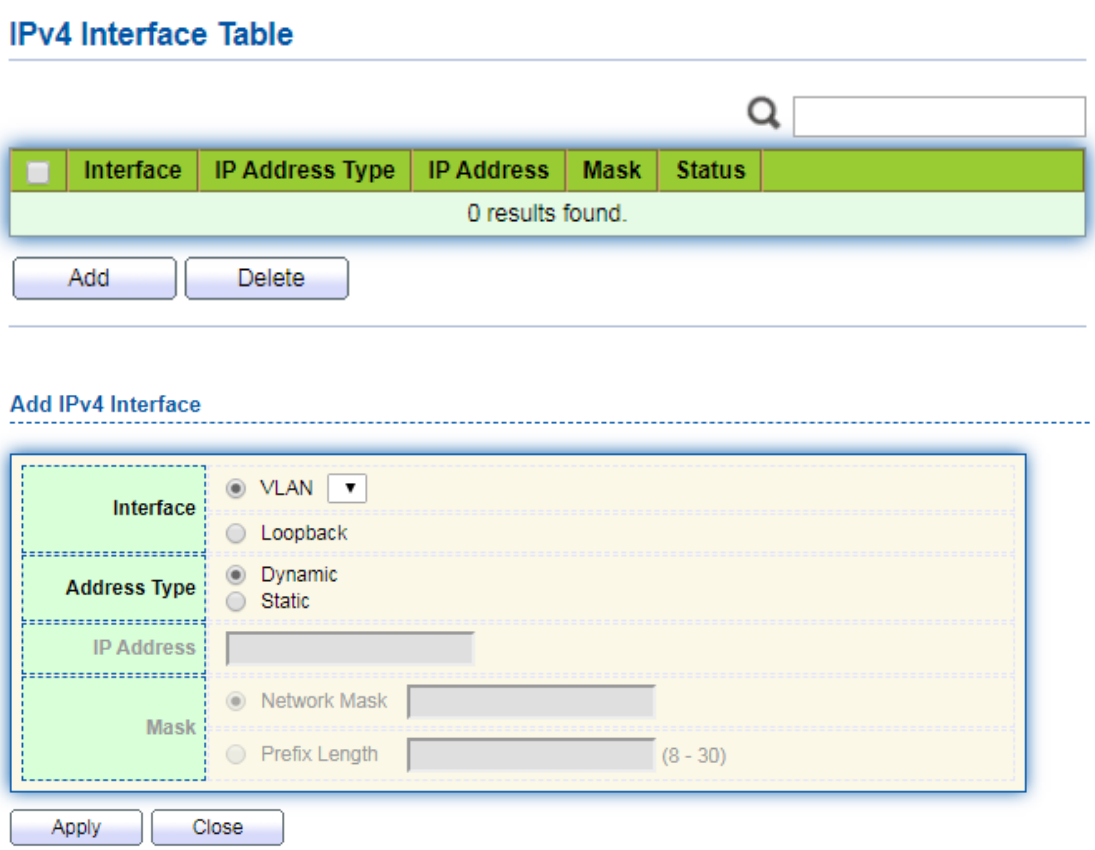
네트워크 레이어 장치와 통신하는 데 사용되는 3 계층 VLAN 인터페이스를 제공합니다. VLANIF 인터페이스는 IP 주소로 구성 할 수 있는 네트워크 계층 인터페이스입니다. VLANIF 인터페이스를 생성하기 전에 해당 VLAN 을 먼저 생성해야합니다. VLANIF 인터페이스의 도움으로 스위치는 다른 네트워크 계층 장치와 통신할 수 있습니다.

13.1 IPv4 Management and Interfaces

13.1.1 IPv4 Interface

Instructions:

1. 탐색 트리에서 “Routing > IPv4 Management and Interfaces > IPv4 Interface”을 선택하고, IPv4 layer 3 interface 설정에 들어갑니다:



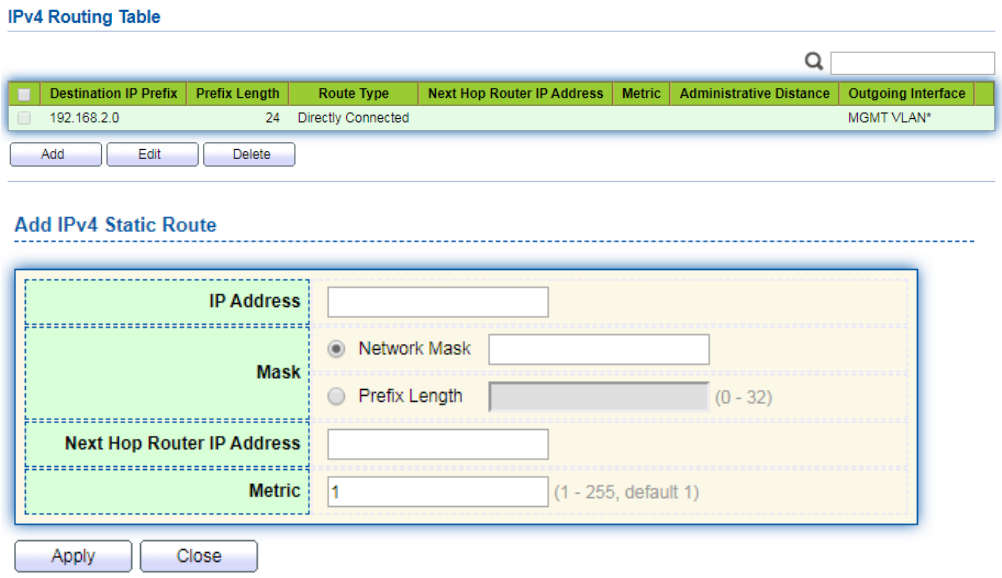
구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	VLAN ID
Loopback	Loopback 인터페이스
Address Type	Dynamic: 인터페이스의 IP 주소를 DHCP 에서 얻습니다. Static: 인터페이스의 IP 주소를 수동으로 입력합니다.
IP Address	인터페이스의 IP 주소
Mask	인터페이스의 IP 주소의 netmask

13.1.2 IPv4 Routes

Instructions:

1. 탐색 트리에서 “Routing > IPv4 Management and Interfaces > IPv4 Routes”을 선택하고, IPv4 static route interface 설정 화면에 들어갑니다:



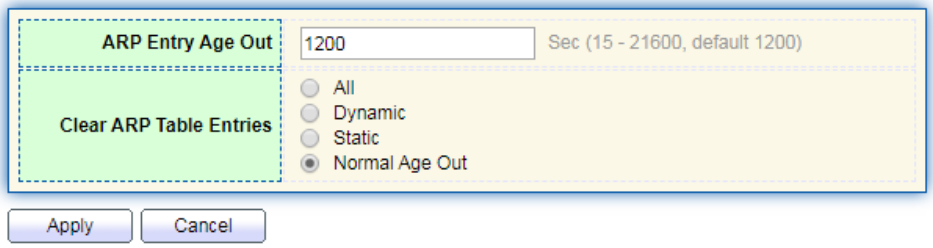
구성 항목은 다음과 같습니다.

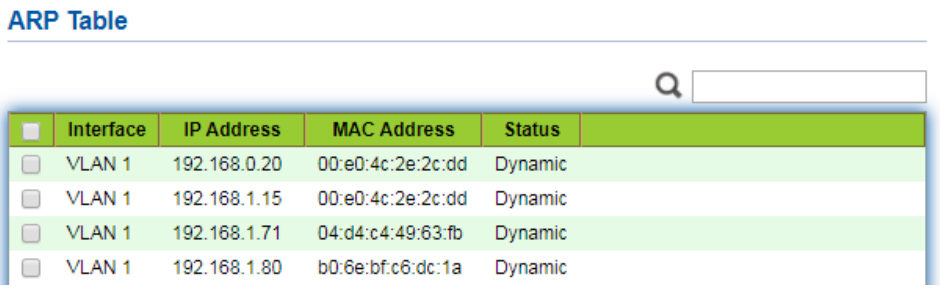
구성 항목	설명
IP Address	목적지 IP 세그먼트
Mask	목적지 IP 마스크
Next Hop Router IP Address	다음 홉 라우터의 IP 주소
Metric	네트워크 홉 카운트

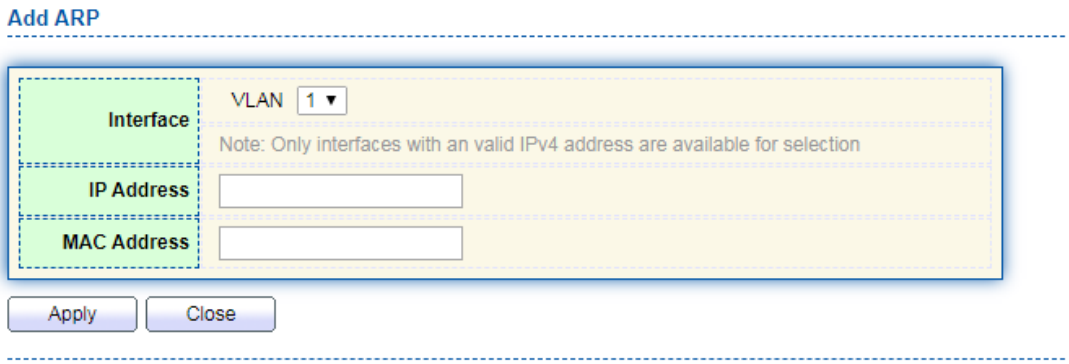
13.1.3 ARP

Instructions:

1. 탐색 트리에서 “Routing > IPv4 Management and Interfaces >ARP”을 선택하고, ARP table entries 설정합니다:







구성 항목은 다음과 같습니다.

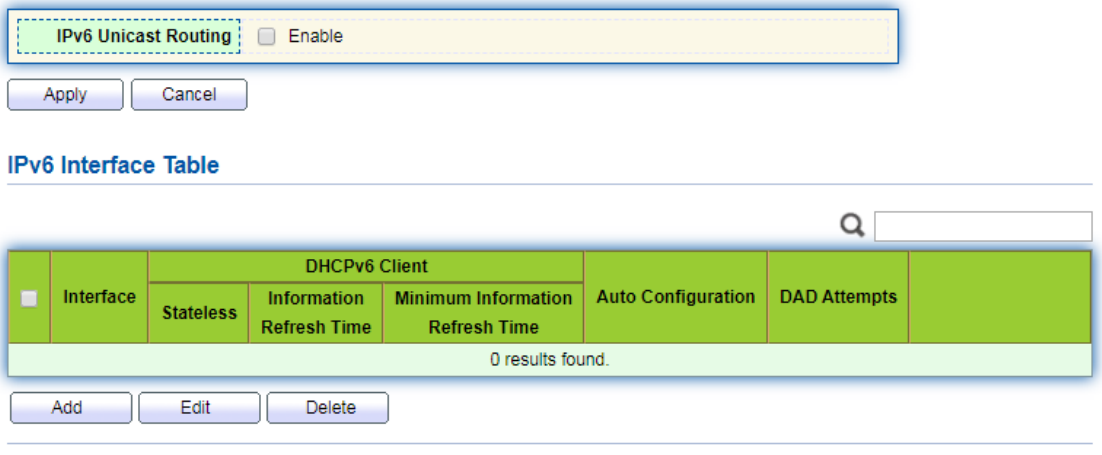
구성 항목	설명
Interface	VLANIF 인터페이스
IP Address	인터페이스 게이트웨이와 동일한 네트워크 세그먼트의 IP 주소
MAC Address	IP 주소에 해당하는 MAC 주소

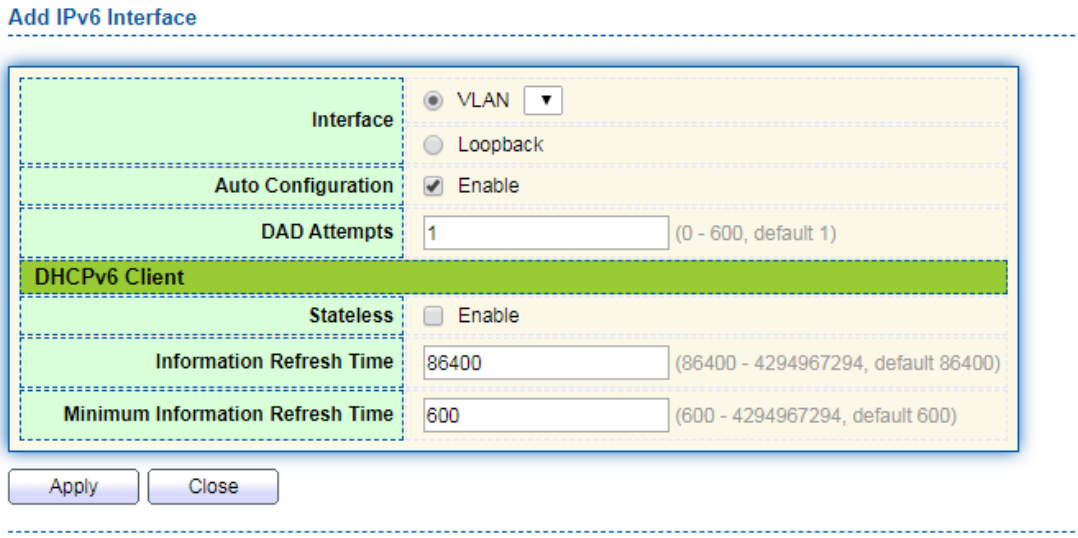
13.2 IPv6 Management and Interfaces

13.2.1 IPv6 Interface

Instructions:

1. 탐색 트리에서 “Routing > IPv6 Management and Interfaces > IPv6 Interface”을 선택하고, IPv6 layer 3 interface 설정에 들어갑니다:





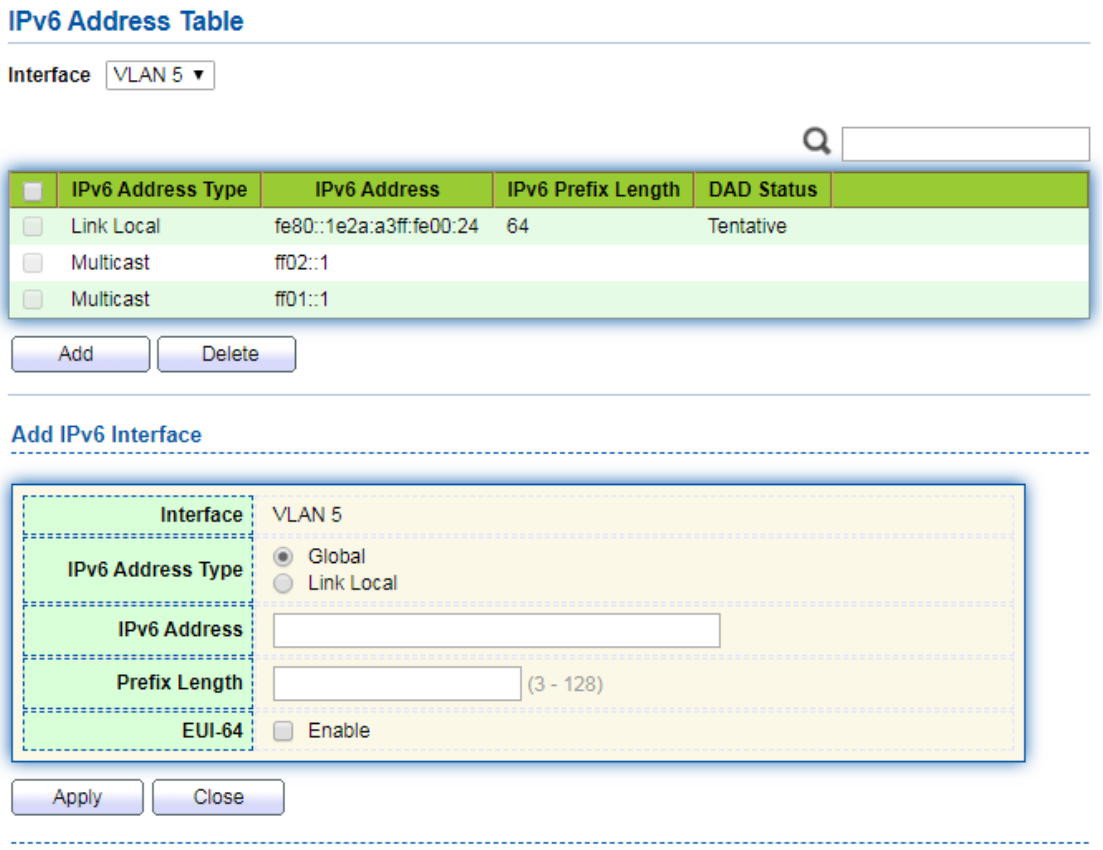
구성 항목은 다음과 같습니다.

구성 항목	설명
VLAN	VLAN ID
Loopback	Loopback 인터페이스
Auto Configuration	자동 설정 스위치
DAD Attempts	중복 주소 감지(duplicate address detection)를 위해 이웃 요청 메시지가 전송되는 횟수 설정
Stateless	Stateless 자동 구성
Information Refresh Time	자동 구성 갱신 시간
Minimum Information Refresh Time	자동 구성을 위한 최소 갱신 시간

13.2.2 IPv6 Address

Instructions:

1. 탐색 트리에서 “Routing > IPv6 Management and Interfaces > IPv6 Address”을 선택하고, IPv6 address 설정에 들어갑니다:



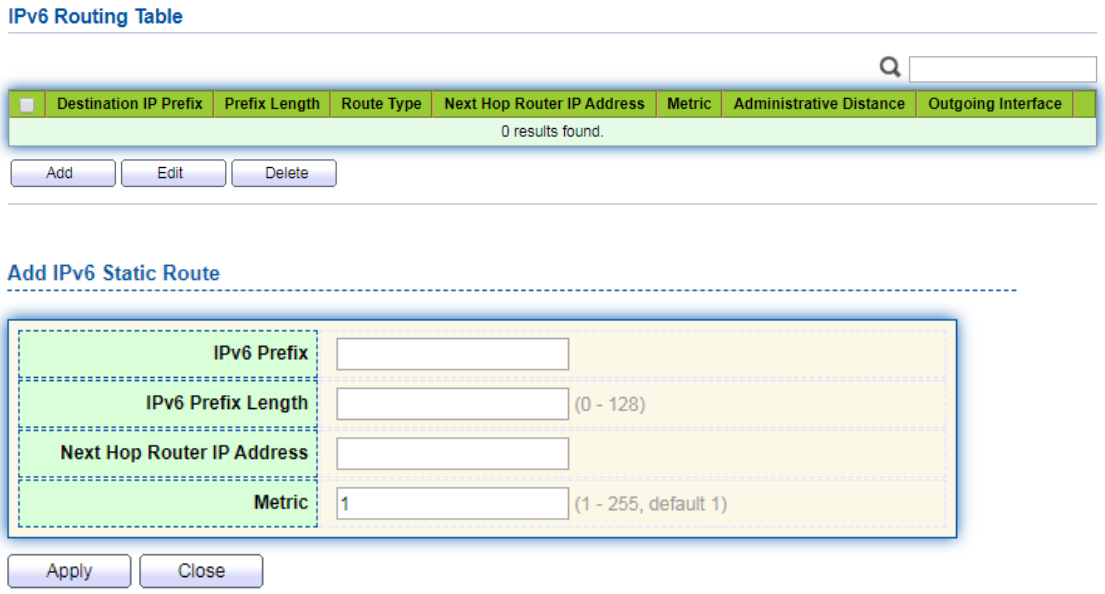
구성 항목은 다음과 같습니다.

구성 항목	설정
Interface	VLANIF 설정
IPv6 Address Type	Global: Global IPv6 address Link Local: Local IPv6 address
IPv6 Address	IPv6 address
Prefix Length	Prefix of IPv6 address
EUI-64	EUI-64 활성화 또는 비활성화

13.2.3 IPv6 Routes

Instructions:

1. 탐색 트리에서 “Routing > IPv6 Management and Interfaces > IPv6 Routes”을 선택하고, IPv6 static route 설정에 들어갑니다:



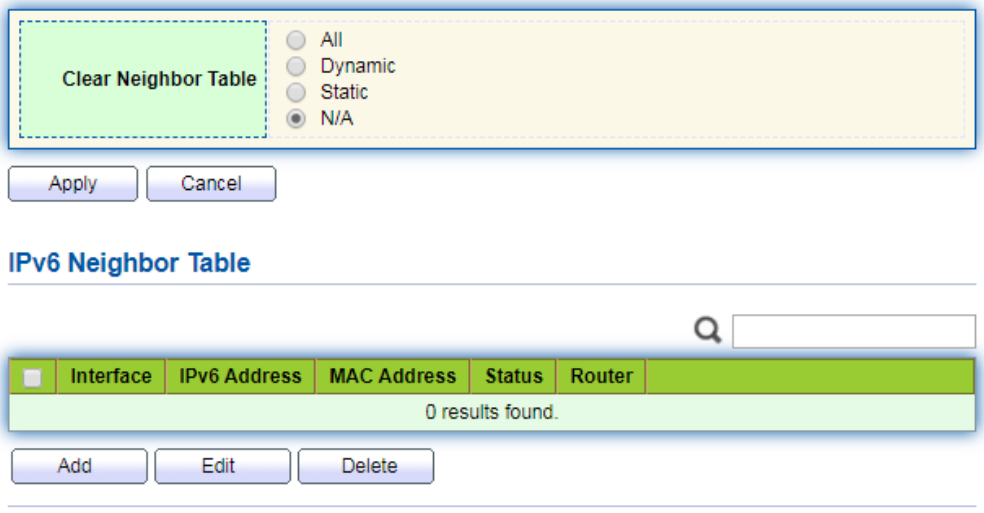
구성 항목은 다음과 같습니다.

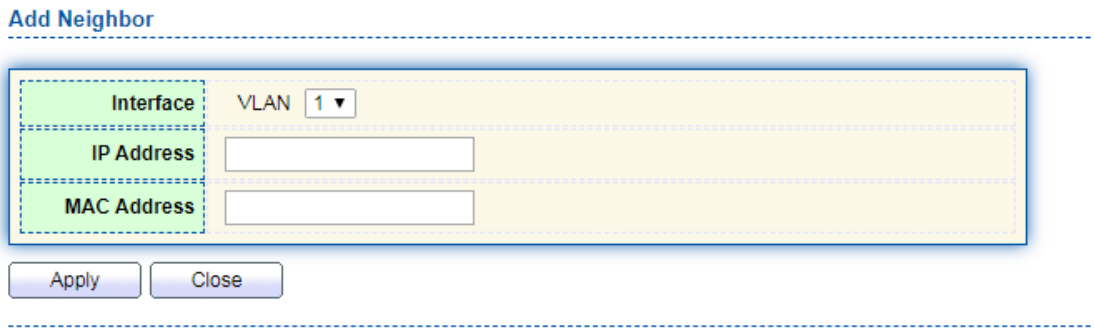
구성 항목	설명
IPv6 Prefix	목적지 IPv6 address segment
IPv6 Prefix Length	목적지 IPv6 address prefix
Next Hop Router IP Address	다음 홉 라우터의 IP 주소
Metric	네트워크 홉 카운트

13.2.4 Neighbors

Instructions:

1. 탐색 트리에서 “Routing > IPv6 Management and Interfaces > Neighbors”을 선택하고, IPv6 neighbor table을 설정하고 확인합니다:





구성 항목은 다음과 같습니다.

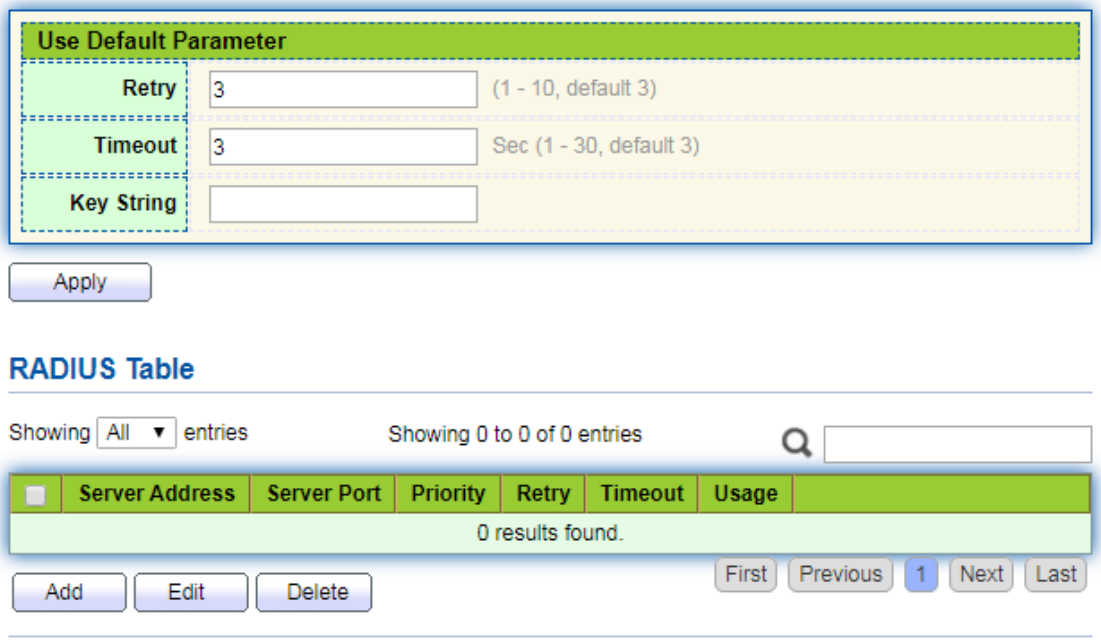
구성 항목	설명
Interface	VLANIF 인터페이스
IP Address	같은 네트워크 세그먼트의 IPv6 address
MAC Address	IPv6 address 에 해당하는 MAC address

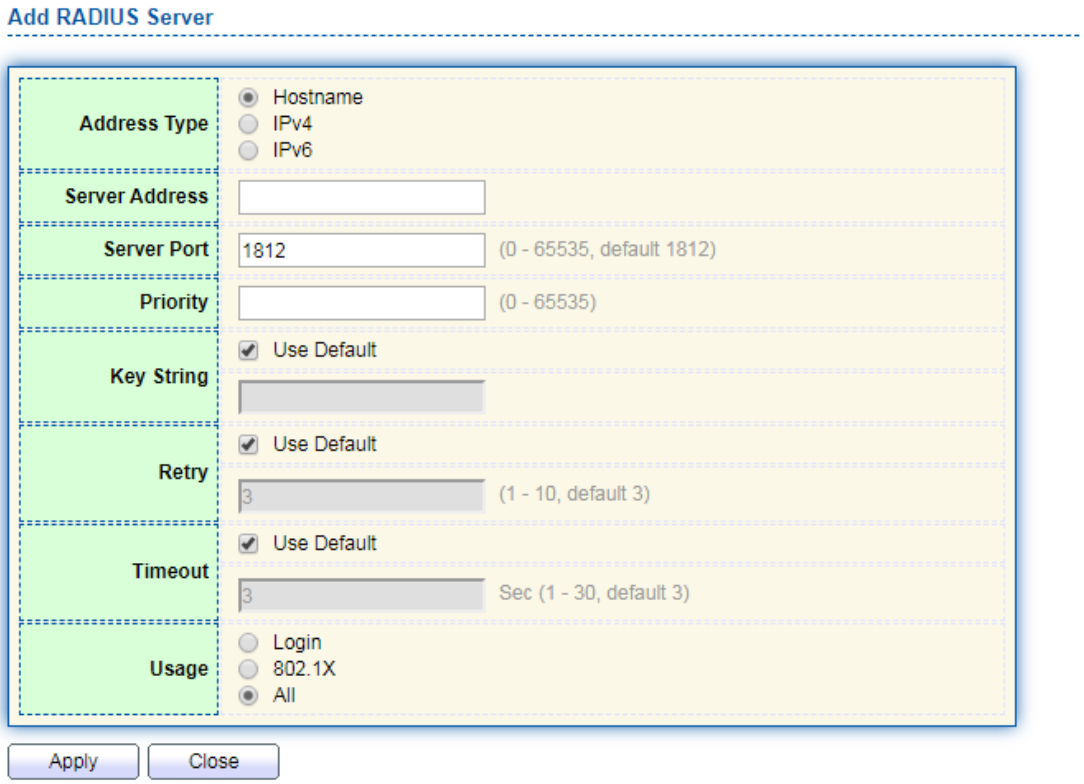
14 Security

14.1 RADIUS

Instructions:

1. 탐색 트리에서 “Security > RADIUS”을 선택하고, RADIUS 설정에 들어갑니다:





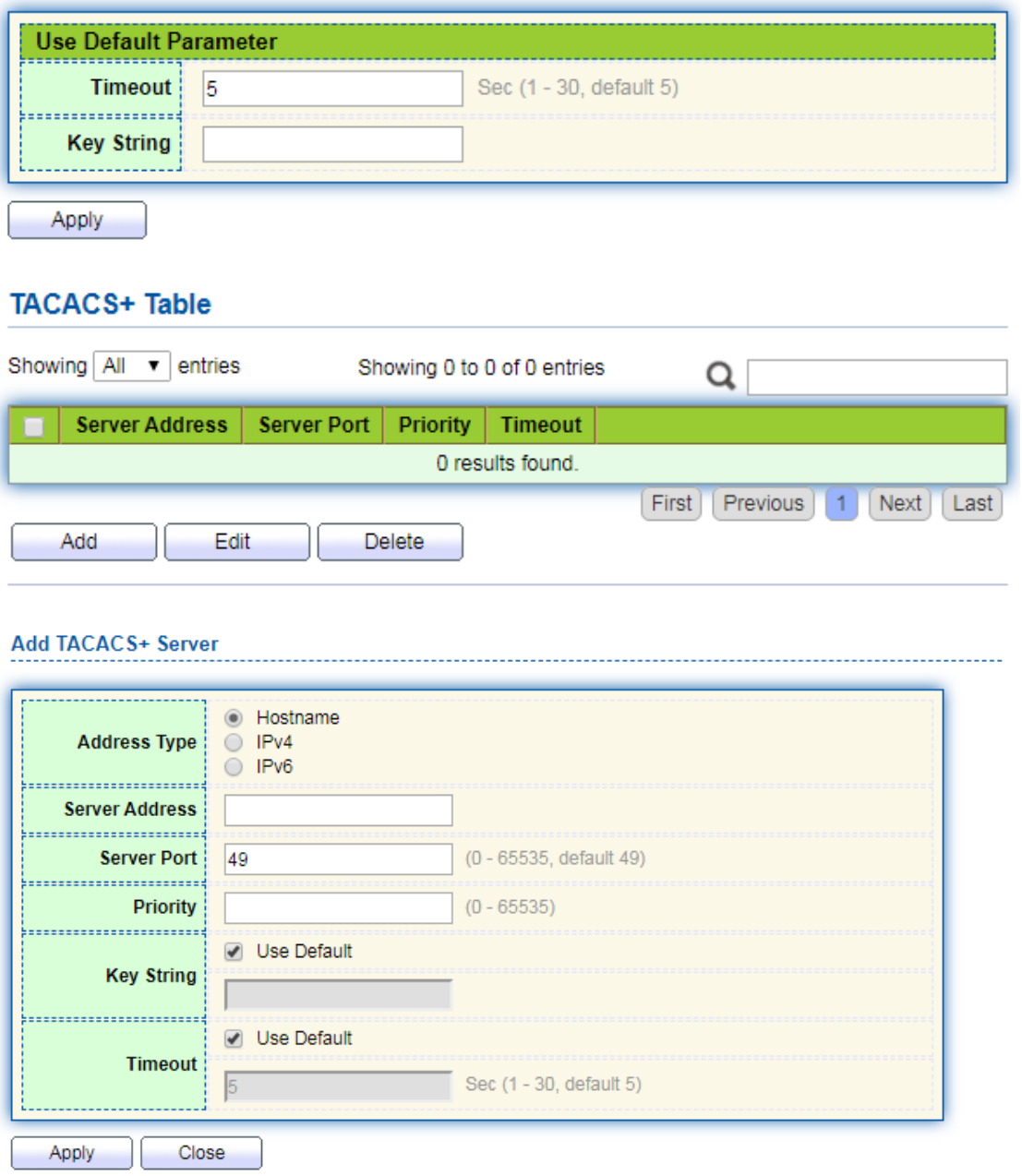
구성 항목은 다음과 같습니다.

구성 항목	설명
Address Type	유형에 따라 호스트 이름, IPv4, IPv6 를 선택할 수 있습니다.
Server Address	서버의 IP address
Server Port	서버 포트
Priority	서비스 priority
Key String	secret key(RADIUS 서버와 스위치 간에 공유)
Retry	재전송 횟수
Timeout	요청 재전송 전에 RADIUS 서버의 응답을 기다리는 시간
Usage	사용 시나리오

14.2 TACACS+

Instructions:

1. 탐색 트리에서 “Security > TACACS+”을 선택하고, TACACS+ 설정 화면에 들어갑니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
Address Type	유형에 따라 호스트 이름, IPv4, IPv6 를 선택할 수 있습니다.
Server Address	서버의 IP address
Server Port	서비스 port
Priority	서비스 priority
Key String	secret key(서버와 스위치 간에 공유)

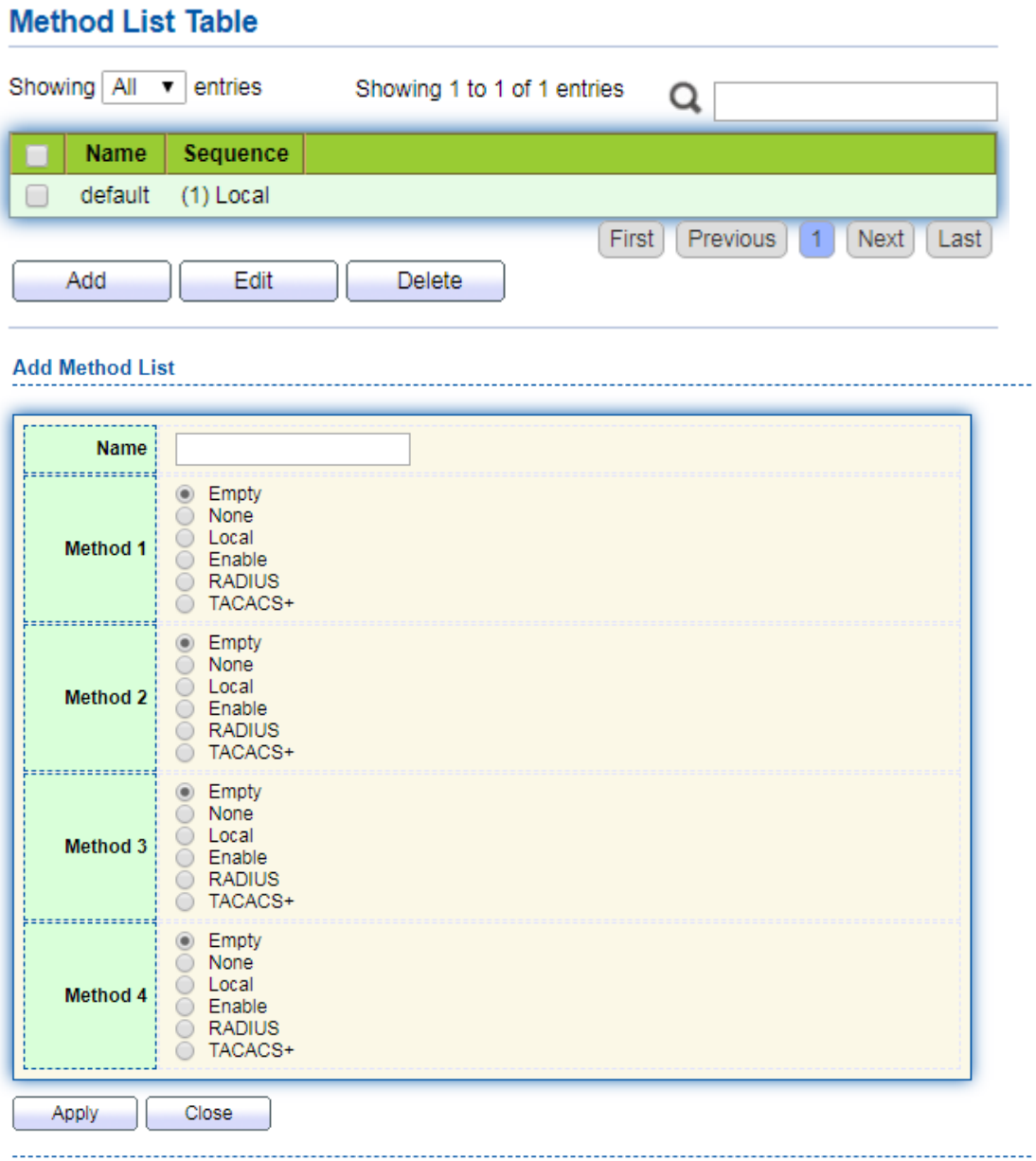
Retry	재전송 횟수
Timeout	요청 재전송 전에 서버의 응답을 기다리는 시간

14.3 AAA

14.3.1 Method List

Instructions:

1. 탐색 트리에서 “Security > AAA > Method List”을 선택하고, method list 에 들어갑니다:



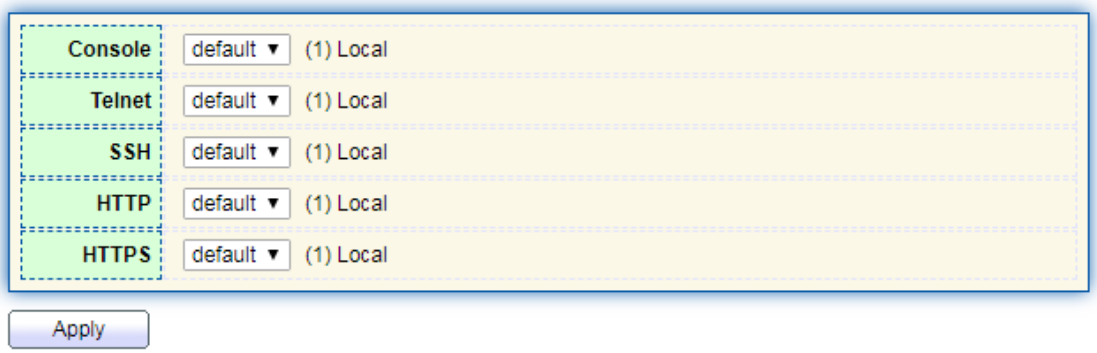
구성 항목은 다음과 같습니다.

구성 항목	설명
Name	Method 이름
Method 1-4	Empty: Method 비활성화 None: 아무 작업 없이 사용자가 인증되도록 합니다. Local: 로컬 사용자 계정 데이터베이스를 사용하여 인증되도록 합니다. Enable: 로컬 활성화 암호 데이터베이스를 사용하여 인증합니다. RADIUS: 원격 RADIUS 서버를 사용하여 인증합니다. TACACS+: 원격 TACACS+ 서버를 사용하여 인증합니다.

14.3.2 Login Authentication

Instructions:

1. 탐색 트리에서 “Security > AAA > Login Authentication”을 선택하고, login authentication 화면에 들어갑니다:

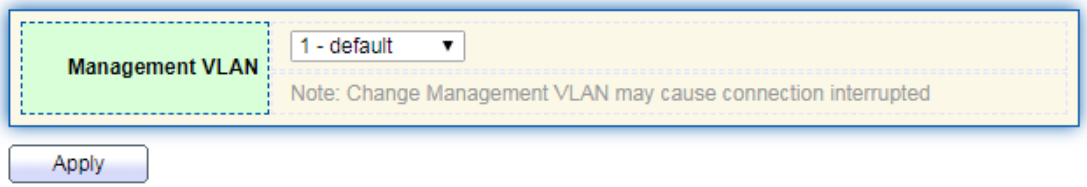


14.4 Management Access

14.4.1 Management VLAN

Instructions:

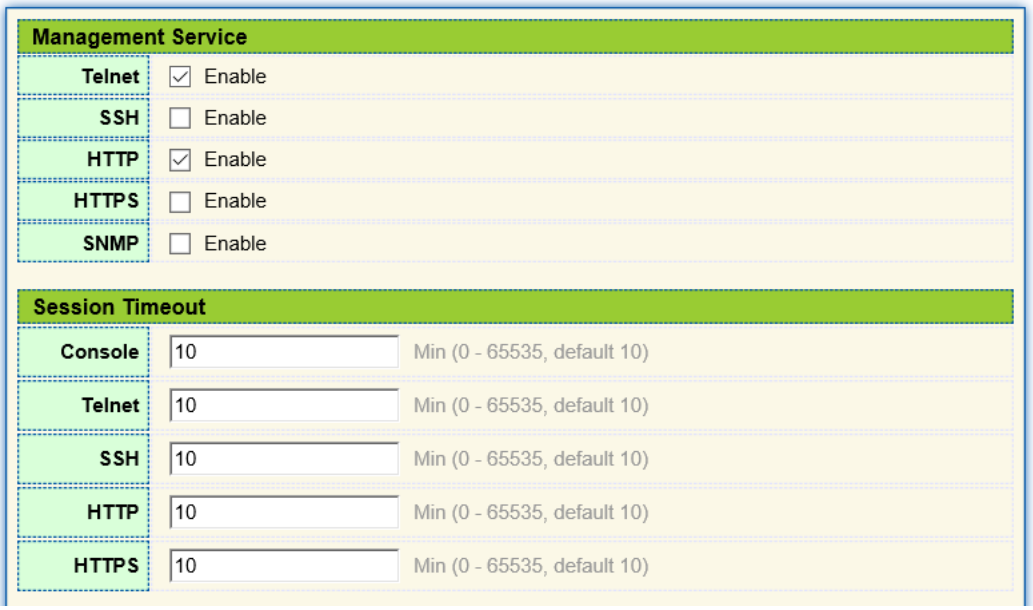
1. 탐색 트리에서 “Security > Management Access > Management VLAN”을 선택하고, management VLAN 에 들어갑니다:



14.4.2 Management Service

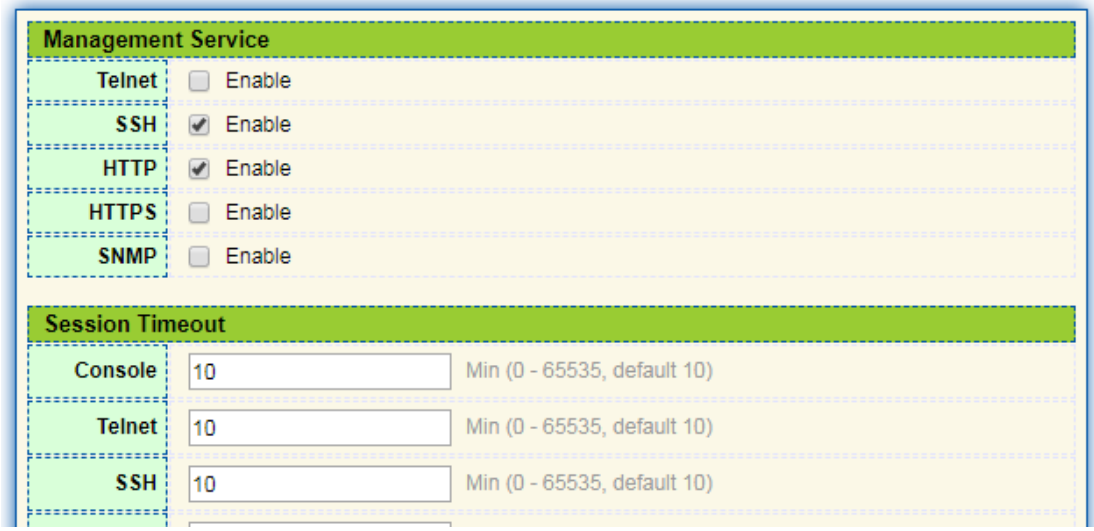
Telnet 서비스 설정 방법:

1. 탐색 트리에서 "Security > Management Access > Management Service"를 선택하고, management service 에 들어갑니다:



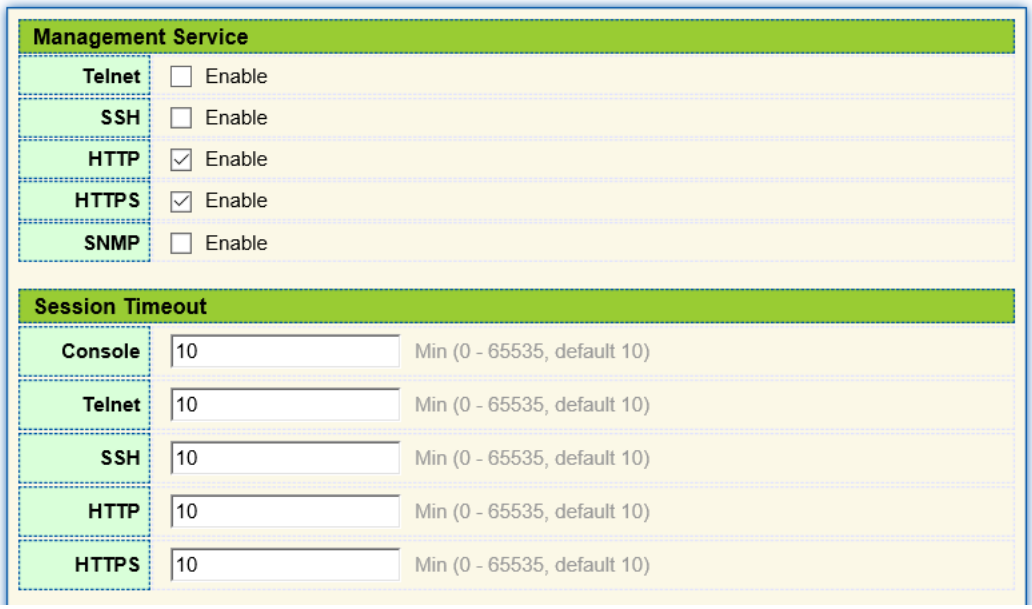
SSH 서비스 설정 방법:

2. 탐색 트리에서 "Security > Management Access > Management Service"을 선택하고, management service 에 들어갑니다.



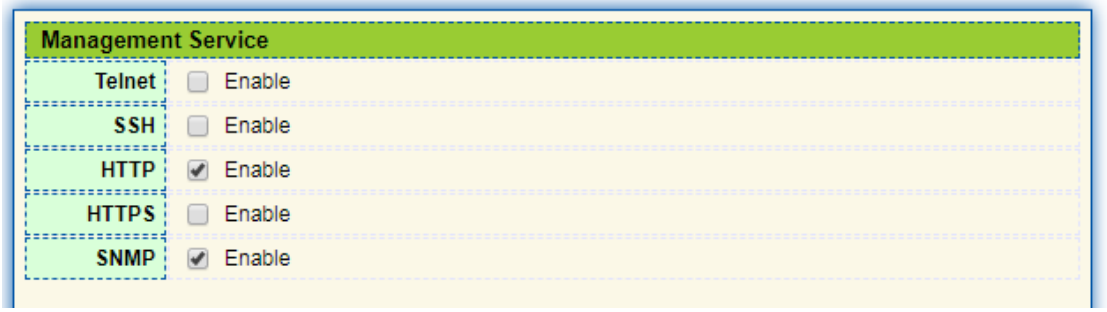
HTTPS 서비스 설정 방법:

3. 탐색 트리에서 "Security > Management Access > Management Service"을 선택하고, management service 에 들어갑니다:



SNMP 서비스 설정 방법:

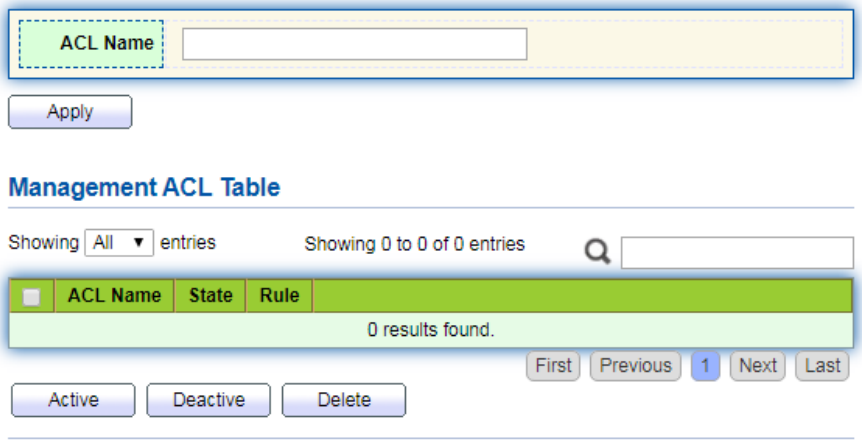
4. 탐색 트리에서 "Security > Management Access > Management Service"을 선택하고, management service 에 들어갑니다:



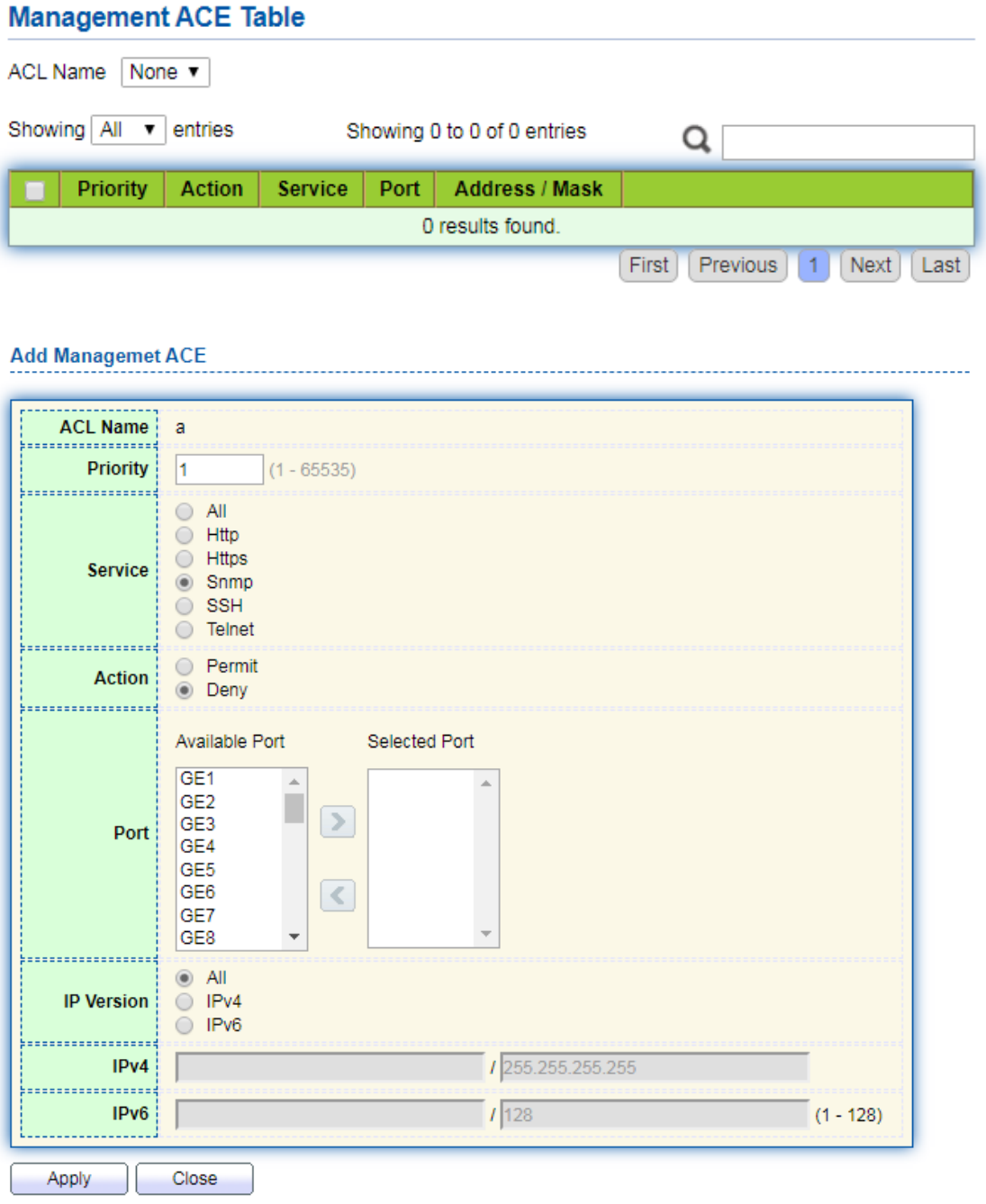
14.4.3 Management ACL

Management 서비스에 ACL 적용 방법:

1. 탐색 트리에서 "Security > Management Access > Management ACL"을 선택하고, management ACL 에 들어갑니다:



2. 탐색 트리에서 “Security > Management Access > Management ACE”, enter management ACE interface as follows:



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	ACL 이름
Priority	ACL Priority

Service	서비스 타입
Action	Match action
Port	ACL 이 적용될 포트
IP Version	IP Address 버전
IPv4	IPv4 address
IPv6	IPv6 address

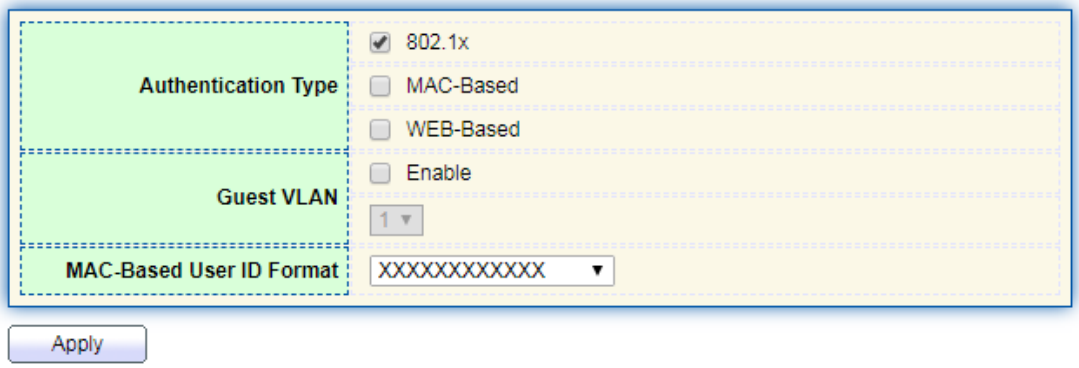
14.5 Authentication Manager

14.5.1 Property

802.1x / MAC / WEB 인증 네트워크 액세스 제어의 Global 설정을 활성화합니다.

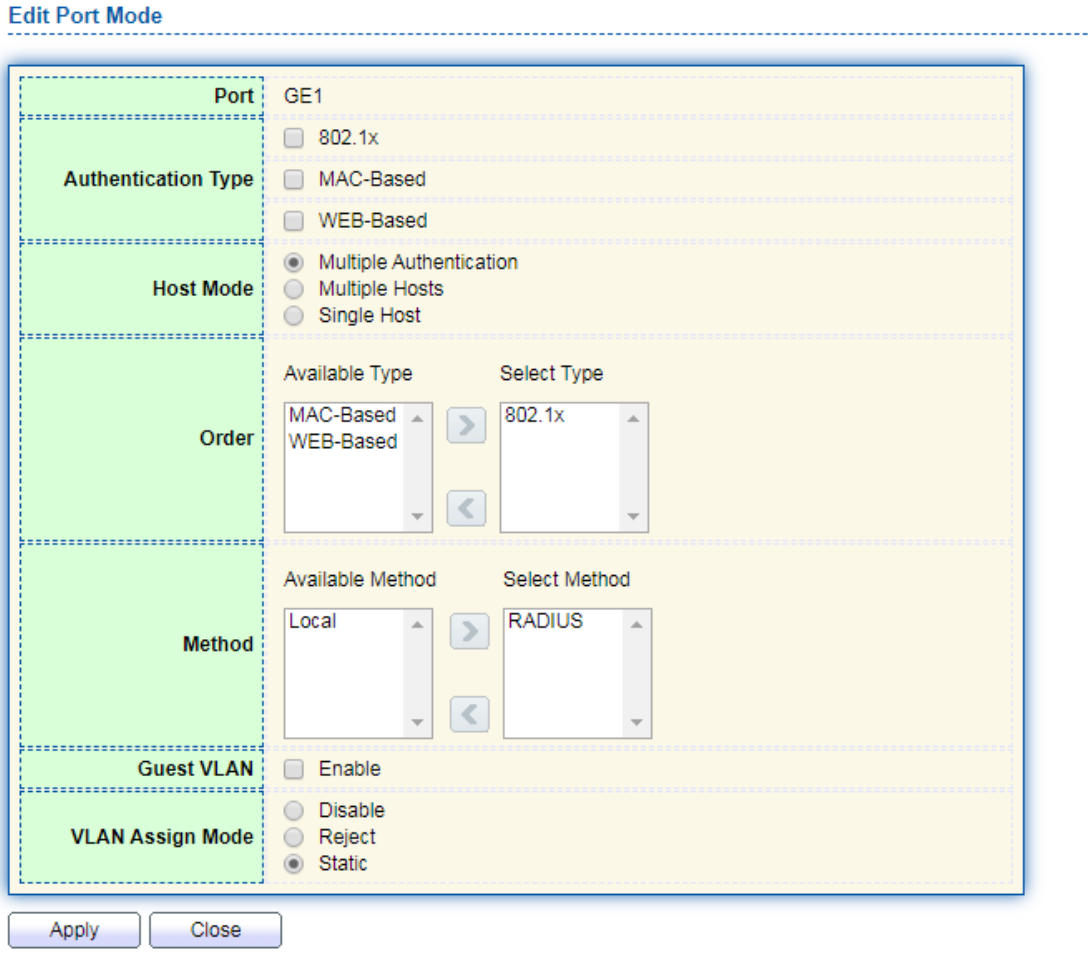
Instructions:

1. 탐색 트리에서 “Security > Management Manager > Property”을 선택하고, global 설정에 들어갑니다:



Port Mode Table

Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
		802.1x	MAC-Based	WEB-Based					
1	GE1	Enabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static



구성 항목은 다음과 같습니다.

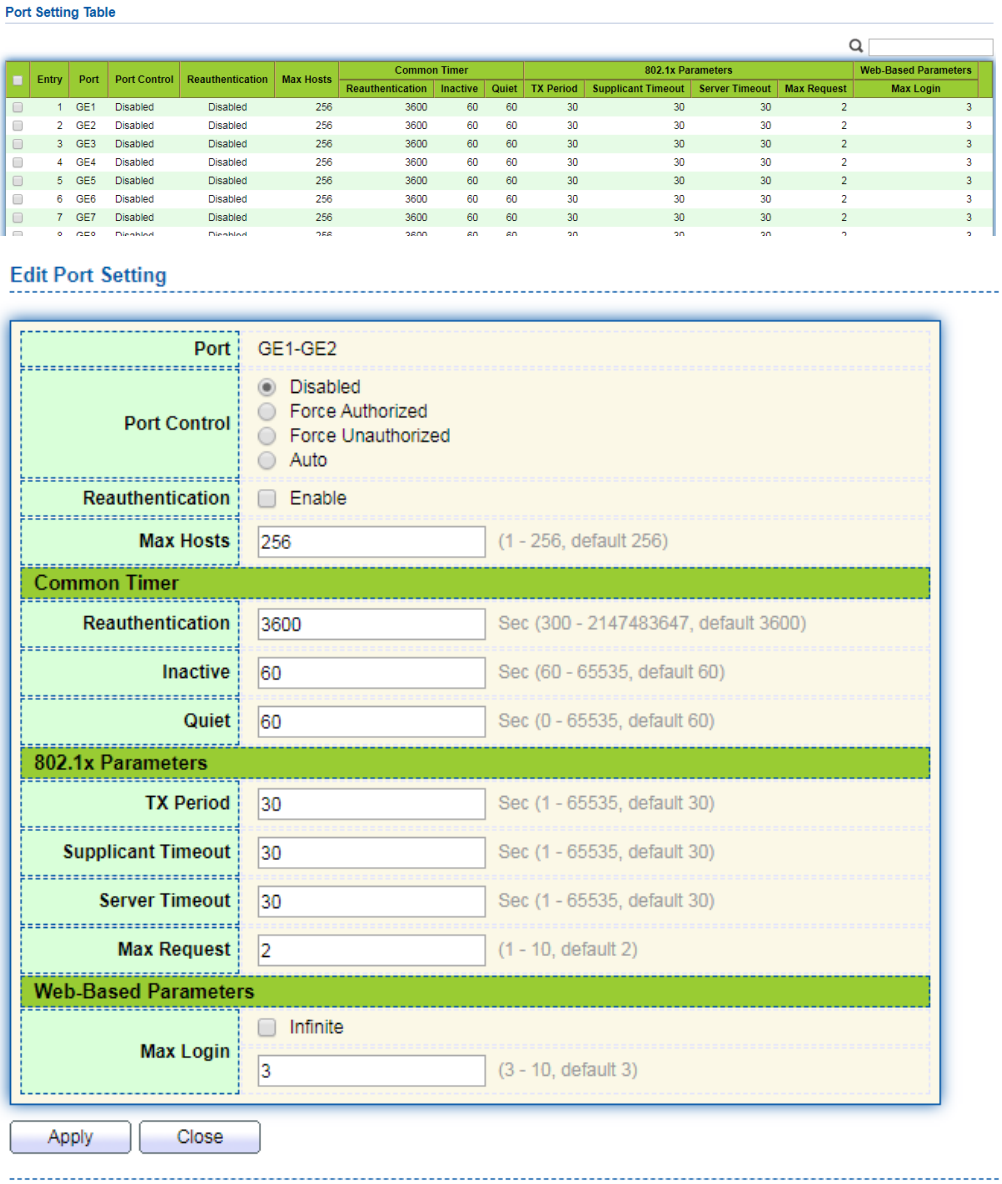
구성 항목	설명
Port	Port 목록
Authentication Type	Port authentication type
Host Mode	Multiple Authentication: 이 모드에서는 모든 클라이언트가 개별적으로 인증 절차를 통과해야합니다. Multiple Hosts: 이 모드에서는 하나의 클라이언트 만 인증하면되고 다른 클라이언트는 동일한 액세스 권한을 갖게됩니다. Single Host: 이 모드에서는 하나의 호스트 만 인증 할 수 있습니다. 최대 호스트 수가 1 로 구성된 다중 인증 모드와 동일합니다.
Order	Match action
Method	포트 인증 method

Guest VLAN	Guest VLAN
VLAN Assign Mode	포트 RADIUS VLAN 할당 모드 Reject : VLAN 인증 정보를 얻으면 사용하십시오. 그러나 VLAN 인증 정보가없는 경우 호스트를 거부하고 권한이없는 상태로 만듭니다. Static : VLAN 인증 정보를 얻으면 사용하십시오. VLAN 인증 정보가없는 경우 호스트의 원래 VLAN 을 유지합니다.

14.5.2 Port Setting

Instructions:

1. 탐색 트리에서 “Security > Management Manager > Port Setting”을 선택하고, port setting 에 들어갑니다:



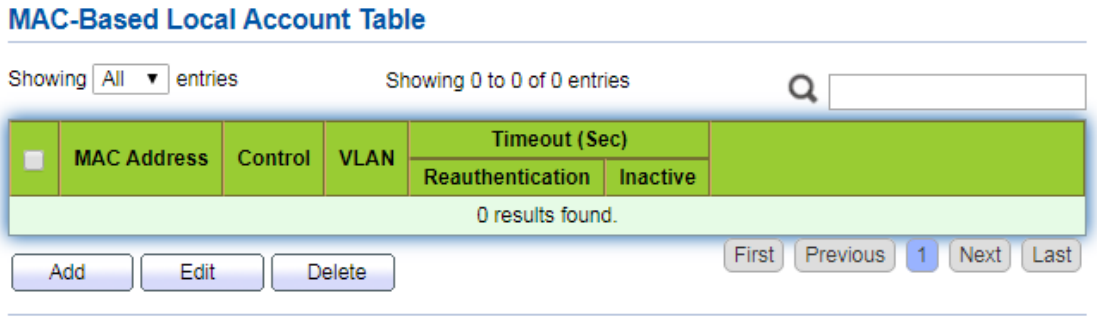
구성 항목은 다음과 같습니다.

구성 항목	설명
Port	Port 목록
Port Control	Force Authorized: 포트가 강제 인증되고 모든 클라이언트가 네트워크에 액세스 할 수 있습니다. Force Unauthorized: 포트가 강제로 승인되지 않습니다. Auto: 네트워크 접근성을 얻기 위해 인증 절차 통과 필요합니다.
Reauthentication	포트 재인증 활성화
Max Hosts	다중 인증 모드의 포트 최대 호스트 수
Reauthentication	로컬 데이터베이스 또는 원격 인증 서버에서 재 인증 시간을 할당하지 않은 경우 포트 재 인증 기간 값 (단위 : 초)
Inactive	포트 비활성 제한 시간 값
Quiet	포트 휴지 기간 값
TX Period	포트 802.1x EAP TX 기간 값
Supplicant Timeout	포트 신청자 시간 초과 값
Server Timeout	포트 802.1x 서버 시간 초과 값
Max Request	포트 802.1x 최대 EAP 요청 값
Max Login	포트 웹 인증 최대 로그인 시도 횟수

14.5.3 MAC-Based Local Account

Instructions:

1. 탐색 트리에서 “Security > Management Manager > MAC-Based Local Account”를 선택하여, 설정에 들어갑니다:

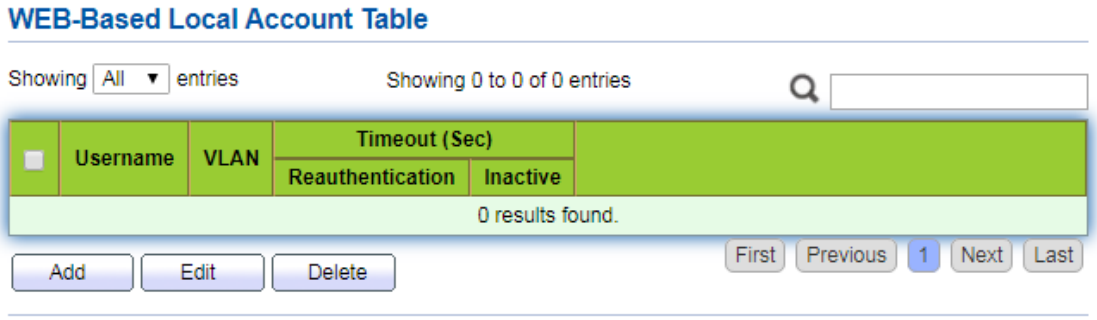


14.5.4 WEB-Based Local Account

Instructions:

1. 탐색 트리에서 “Security > Management Manager > WEB-Based Local Account”를

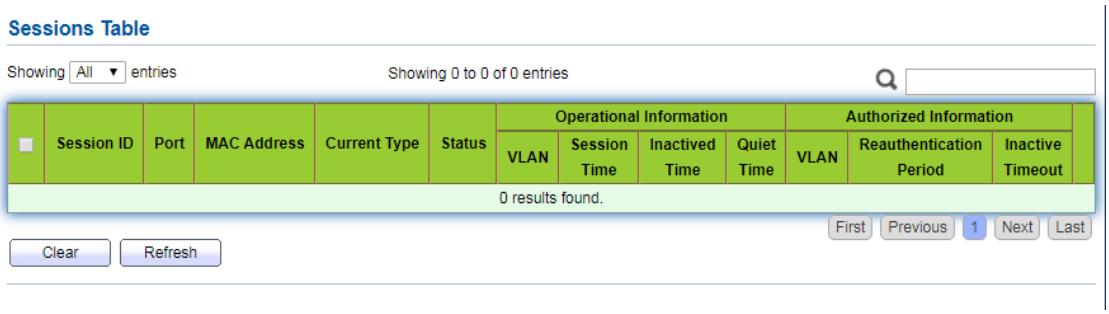
선택하여 설정에 들어갑니다:



14.5.5 Sessions

Instructions:

1. 탐색 트리에서 "Security > Management Manager > Sessions"을 선택하여, session을 확인합니다:



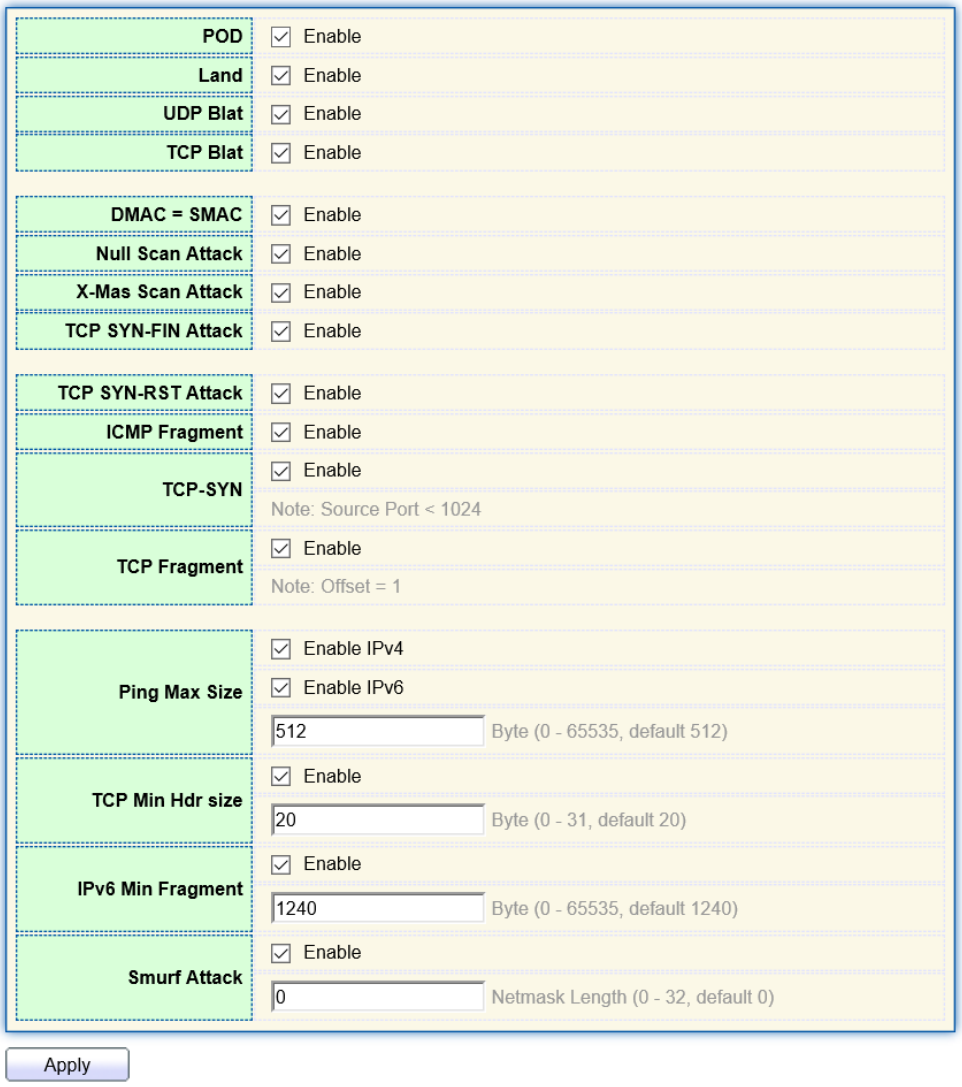
14.6 DoS

14.6.1 Property

DOS 공격 저항 옵션을 활성화하여 스위치를 더 안전하게 만듭니다.

Instructions

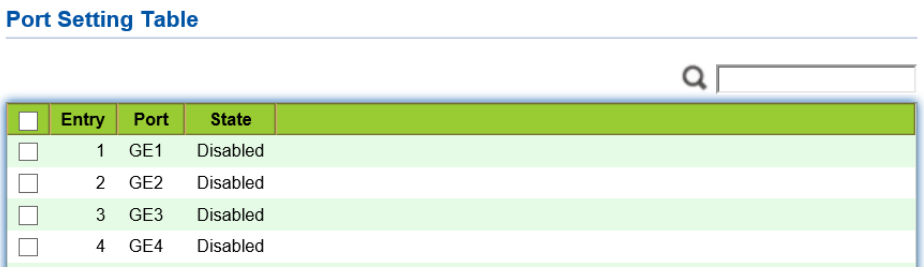
1. 탐색 트리에서 "Security > DoS > Property"를 선택하여 "DoS Global Configuration"에 들어갑니다.



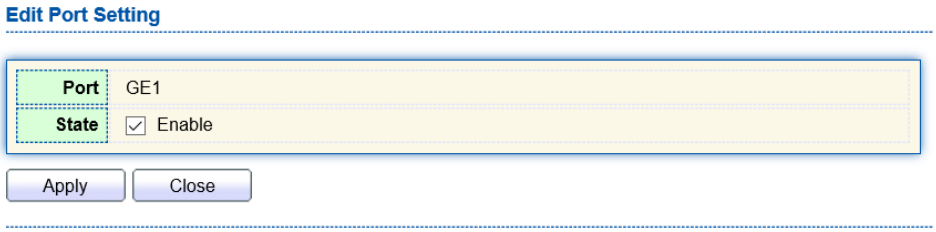
14.6.2 Port Setting

포트 기반으로 DoS 공격 방어를 활성화 합니다.

Instructions
1. 탐색 트리에서 “Security > DoS > Port Setting”를 선택합니다:



2. 포트를 선택하고 “Edit” 하여 DoS 공격 방어를 활성화 합니다.

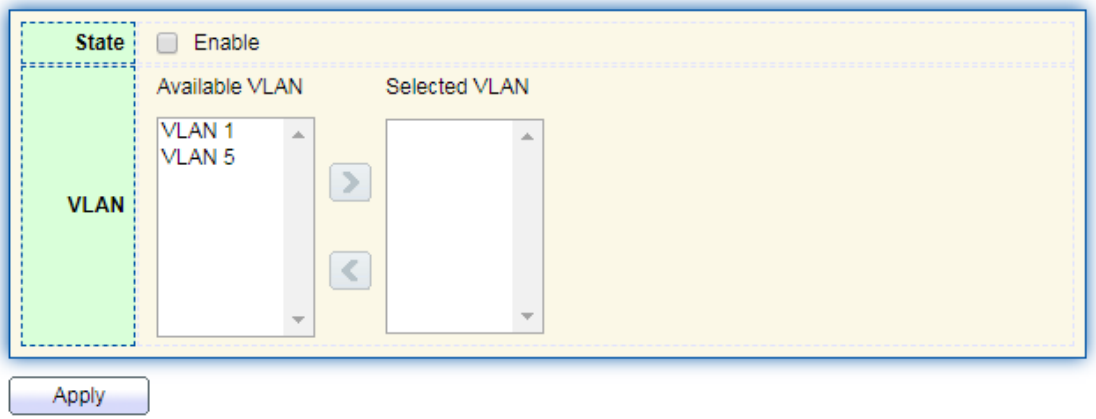


14.7 Dynamic ARP Inspection

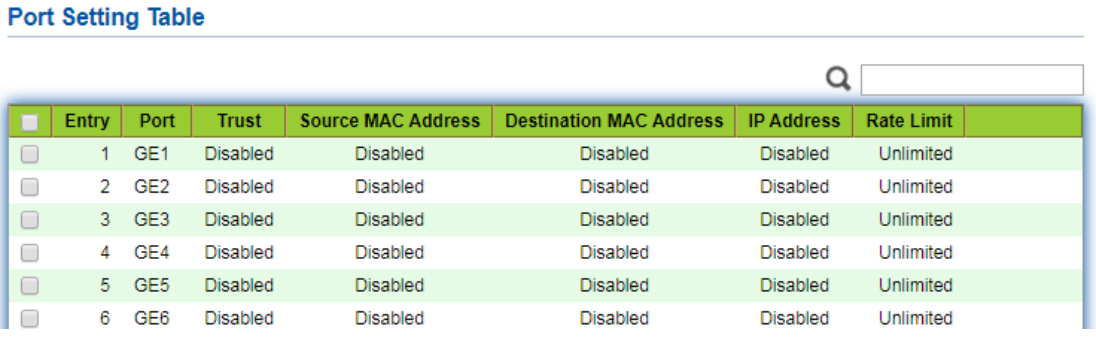
14.7.1 Property

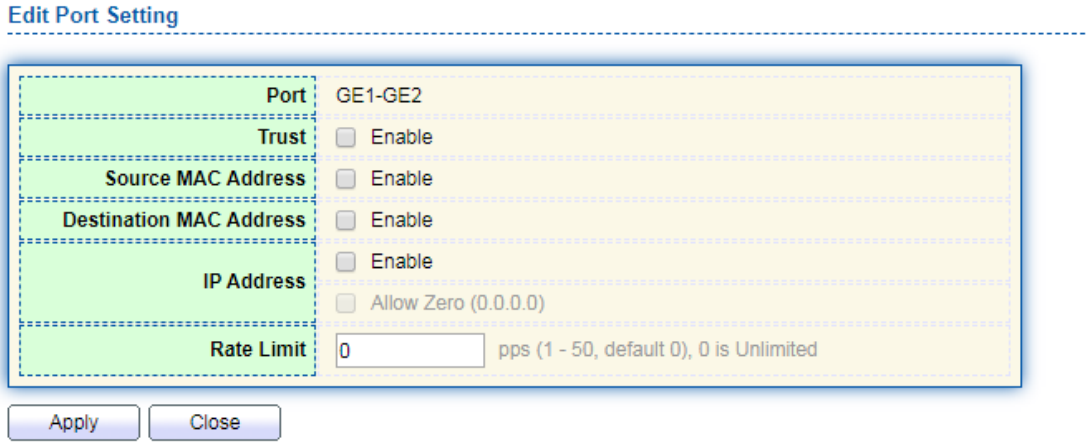
Instructions

1. 탐색 트리에서 “Security > Dynamic ARP Inspection > Property” 을 선택하고, global 설정에 들어갑니다:



2. 포트를 선택하고 “Edit” 하여 포트 설정에 들어갑니다:

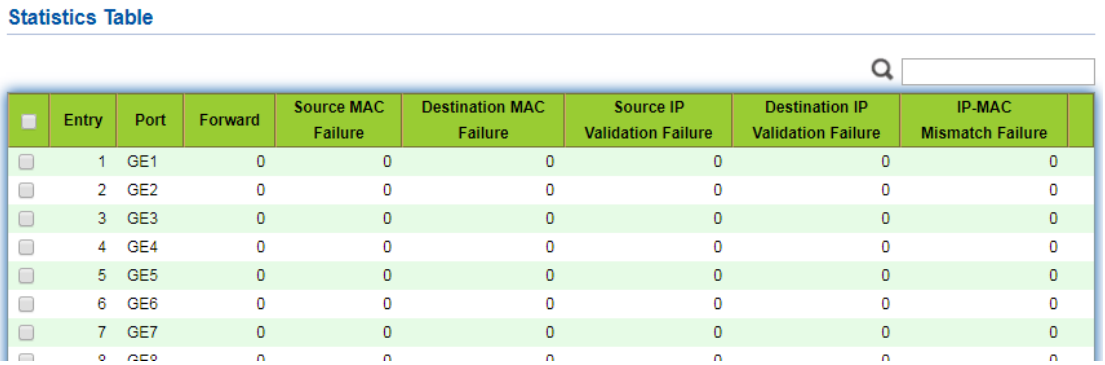




14.7.2 Statistics

Instructions

1. 탐색 트리에서 “Security > Dynamic ARP Inspection > Statistics” 을 선택하고, DAI 통계를 확인합니다:



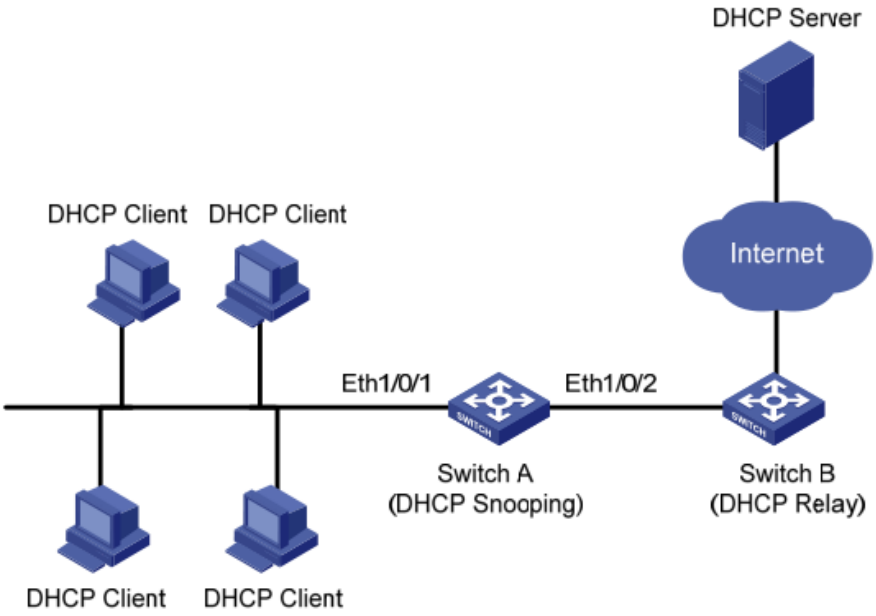
14.8 DHCP Snooping

보안을 위해 네트워크 관리자는 인터넷을 서핑하는 사용자의 **IP** 주소를 기록하고 **DHCP** 서버에서 얻은 **IP** 주소와 호스트의 **MAC** 주소 간의 일치를 확인해야 할 수 있습니다.

스위치는 네트워크 계층에서 보안 **DHCP** 릴레이를 통해 사용자의 **IP** 주소를 기록 할 수 있습니다.

스위치는 데이터 링크 계층에서 **DHCP** 스누핑을 통해 **DHCP** 메시지를 모니터링하고 사용자의 **IP** 주소를 기록 할 수 있습니다. 또한 네트워크의 사설 **DHCP** 서버는 사용자에게 잘못된 **IP** 주소로 이어질 수 있습니다. 사용자가 합법적 인 **DHCP** 서버를 통해 **IP** 주소를 확보 할 수 있도록 **DHCP** 스누핑 보안 메커니즘은 포트를 신뢰 포트와 비 신뢰 포트로 나눕니다

Trust Port 는 합법적 인 **DHCP** 서버를 직접 또는 간접적으로 연결합니다. **DHCP** 클라이언트의 올바른 **IP** 주소를 확인하기 위해 수신 된 **DHCP** 메시지를 전달합니다. **Untrust Port** 는 잘못된 **DHCP** 서버를 연결합니다. 신뢰할 수없는 포트의 **DHCP** 서버에서 수신 한 **DHCPACK** 및 **DHCPOFFER** 메시지는 잘못된 **IP** 주소를 방지하기 위해 폐기됩니다..



DHCP Snooping 의 일반적인 네트워킹

다음 방법은 **DHCP** 서버에서 **IP** 주소 및 사용자 **MAC** 주소를 가져오는 데 사용됩니다:

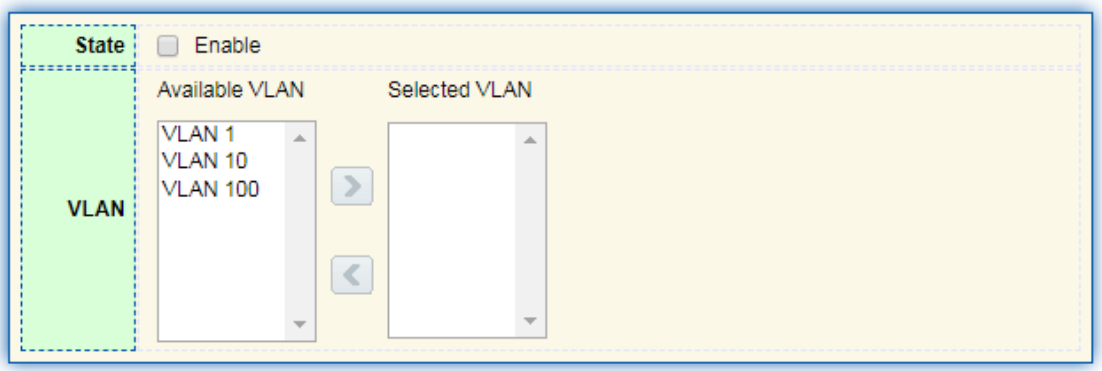
- **DHCPREQUEST** 메시지 스누핑
- **DHCPACK** 메시지 스누핑

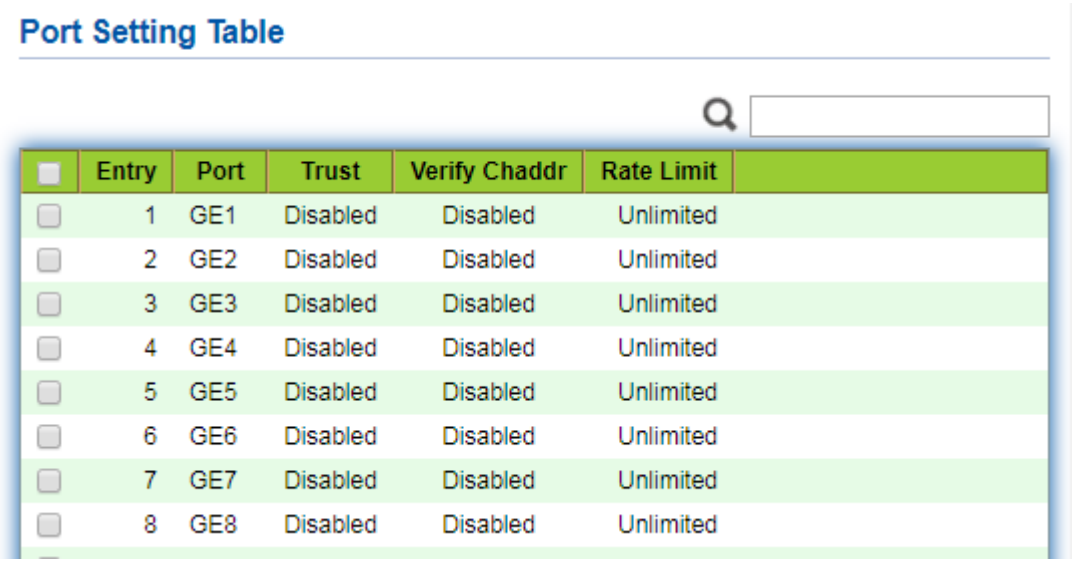
14.8.1 Property

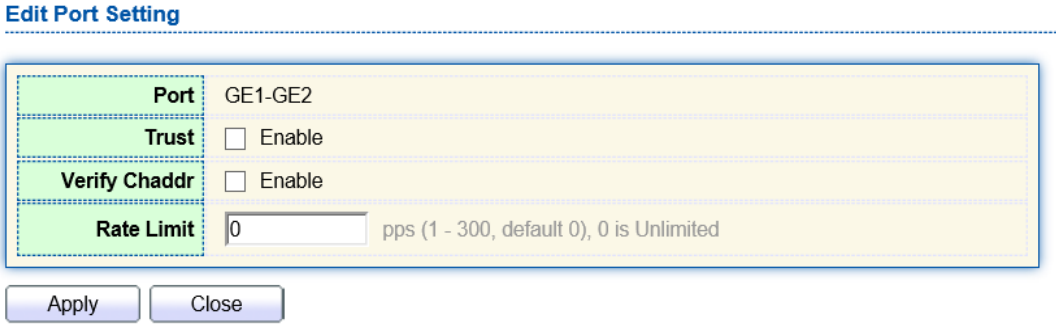
DHCP Snooping 활성화

Instructions:

1. 탐색 트리에서 “Security > DHCP Snooping > Property”을 선택합니다. **DHCP** 스누핑 인터페이스는 글로벌 구성과 포트 구성으로 나뉩니다. 포트 구성에서 수정할 포트를 선택하고 다음과 같이 세부 정보를 수정합니다:





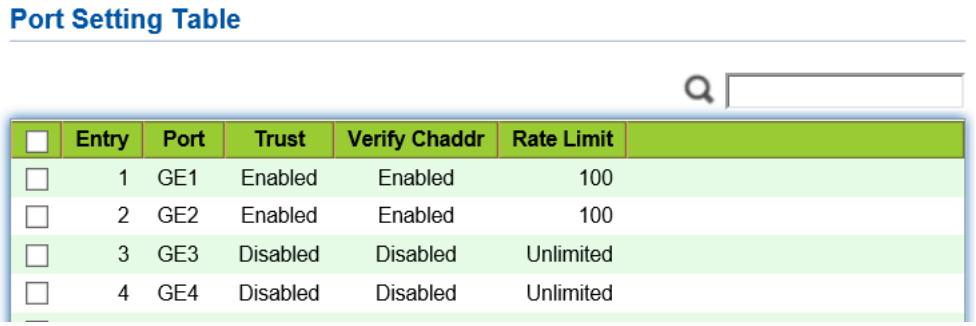


구성 항목은 다음과 같습니다.

구성 항목	설명
State	**DHCP** 스누핑 활성화 및 비활성화
VLAN	**DHCP** 스누핑의 유효한 **VLAN** 번호
Port	**DHCP** 스누핑의 포트 번호 구성
Trust	포트가 신뢰 포트인지 여부

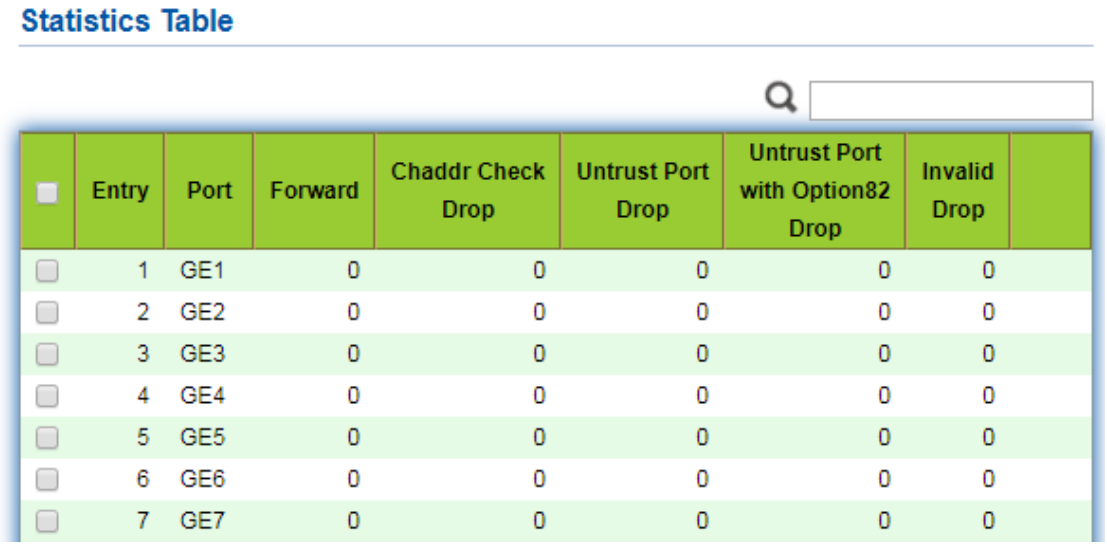
Client Address Inspection	클라이언트 주소에 대한 일관성 검사 사용 여부
Rate Limit	포트가 속도 제한을 활성화하고 값을 구성하는지 여부

2. 해당 구성 항목을 입력합니다.
3. “Apply” 하고 다음과 같이 마칩니다.



14.8.2 Statistics

Instructions
1. 탐색 트리에서 “Security > Dynamic ARP Inspection > Statistics” 을 선택하여, DHCP Snooping 통계를 확인합니다:



14.8.3 Option82 Property

네트워크의 사설 DHCP 서버에 의해 사용자는 잘못된 IP 주소를 얻을 수 있습니다. DHCP 스누핑 보안 메커니즘은 합법적인 DHCP 서버를 통해 IP 주소를 제공하기 위해 포트를 Trust Port 와 Untrust 포트로 나눕니다.

- Trust Port 는 적법한 DHCP 서버를 직간접적으로 연결합니다. 수신된 DHCP

메시지를 전달하여 DHCP 클라이언트의 올바른 IP 주소를 보장합니다.

- Untrust Port 는 불법 DHCP 서버를 연결합니다. 신뢰할 수 없는 포트에서 DHCP 서버가 응답한 DHCP ACK 및 DHCPOFFER 메시지는 잘못된 IP 주소를 방지하기 위해 삭제됩니다.

옵션 82 는 DHCP 클라이언트의 위치를 기록하는 DHCP 메시지의 릴레이 에이전트 정보 옵션입니다. DHCP 릴레이 (또는 DHCP 스누핑 장치)가 DHCP 클라이언트에서 DHCP 서버로 전송된 요청, 메시지를 수신하면 관리자는 옵션 82 를 추가하여 DHCP 클라이언트를 찾고 보안, 비용 등을 제어 할 수 있습니다. 주소 할당에 대한보다 유연한 접근 방식은 다음과 같습니다. IP 주소 및 기타 매개 변수 할당 정책에 따라 옵션 82 를 지원하는 서버에서 생성됩니다.

옵션 82 에는 최대 255 개의 하위 옵션이 포함되어 있습니다. 옵션 82 가 정의된 경우 하나 이상의 하위 옵션이 정의되어야합니다. 현재 장치는 회로 ID 하위 옵션과 원격 ID 하위 옵션의 두 가지 하위 옵션을 지원합니다.

RFC 3046 이 옵션 82 옵션을 균일화하지 못하기 때문에 제조업체는 일반적으로 필요에 따라 옵션을 채웁니다. DHCP 릴레이 장치로서 이더넷 스위치는 옵션 82 하위 옵션에 대한 확장 패딩 형식을 지원하며 패딩 기본값은 다음과 같습니다. :

- 하위 옵션 1 : DHCP 클라이언트가 보낸 요청 메시지를 수신하는 포트의 VLAN 번호 및 포트 인덱스 (포트 물리적 번호에서 1 을 뺀 값).
- 하위 옵션 2 : DHCP Client Request 메시지를 수신하는 DHCP 릴레이 장치의 MAC 주소를 연결합니다.

Option 82 의 DHCP 릴레이 지원 메카니즘

DHCP 클라이언트가 DHCP 릴레이를 통해 DHCP 서버에서 IP 주소를 획득하는 과정은 기본적으로 DHCP 서버에서 직접받는 과정과 동일합니다. 발견, 프로비저닝, 선택 및 검증 단계가 필수적입니다. DHCP 릴레이의 지원 메커니즘은 다음과 같이 소개됩니다. :

(1) DHCP 릴레이는 수신 된 DHCPREQUEST 메시지에서 옵션 82 를 확인하고 그에 따라 처리합니다.

- 기존 옵션 82 메시지의 경우 DHCP 릴레이는 구성 정책 (삭제, 릴레이 옵션 82 로 교체 또는 원래 옵션 82 유지)에 따라 처리 한 다음 DHCP 서버로 전달합니다.
- 옵션 82 가없는 메시지의 경우 DHCP 릴레이는 새 메시지를 DHCP 서버에 추가하고 전달합니다.

(2) DHCP 릴레이는 DHCP 서버에서받은 응답 메시지에서 옵션 82 를 벗겨냅니다..

Description:

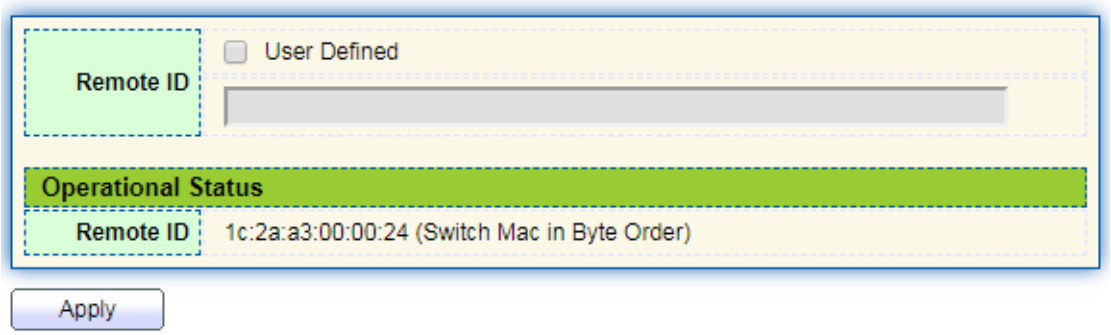
DHCP 클라이언트는 DHCPDISCOVERY 메시지와 DHCPREQUEST 메시지를 전송합니다. DHCP 릴레이는 요청 메시지에 대한 제조업체의 DHCP 서버 처리 메커니즘이 다르기 때문에 두 메시지에 옵션 82 를 추가합니다. 일부 장치는 DHCPDISCOVERY 메시지에서 옵션 82 를 처리하고 다른 장치는 DHCPREQUEST 메시지에서

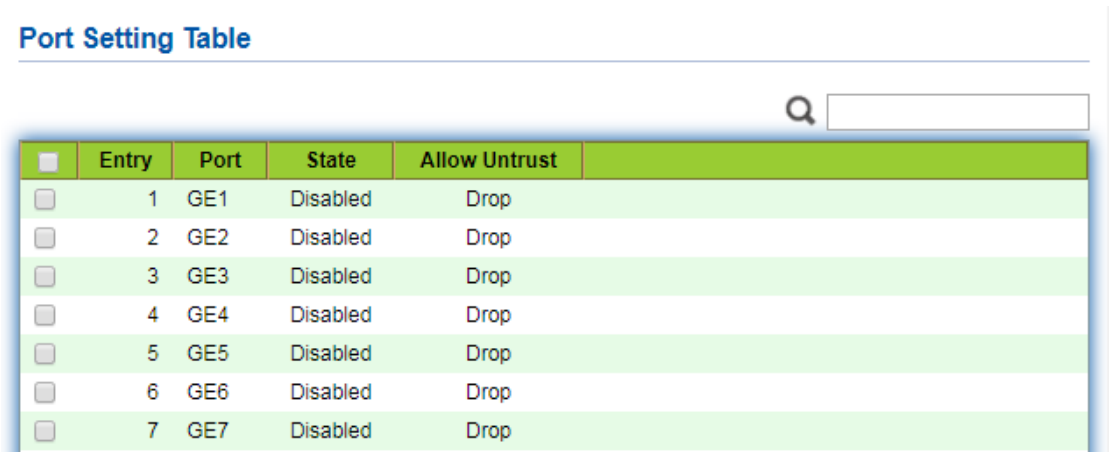
처리합니다.

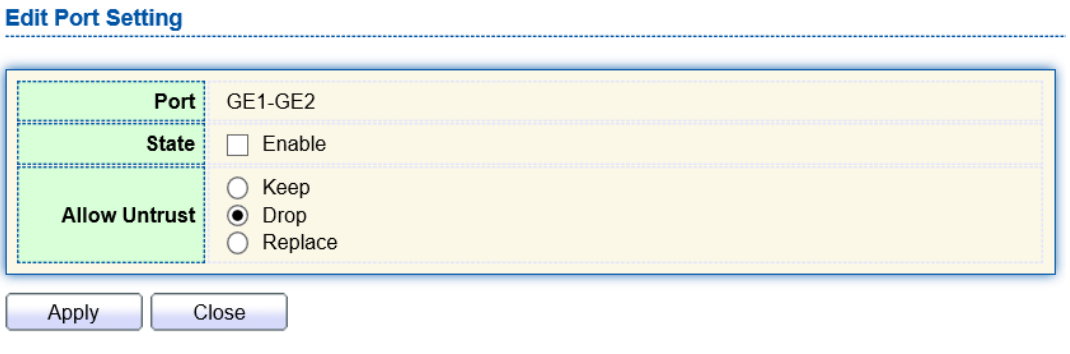
DHCP 스누핑 및 옵션 82 기능으로 구성된 스위치는 DHCP 클라이언트가 보낸 옵션 82 와 함께 DHCPREQUEST 메시지를 수신합니다. DHCP 스누핑은 다양한 구성 처리 전략 및 하위 옵션 내용에 따라 다른 처리 메커니즘을 사용합니다.

Instructions:

1. 탐색 트리에서 “Security > DHCP Snooping > Option82 Property”을 선택하고, 포트를 선택한 다음 “Edit”합니다.







구성 항목은 다음과 같습니다.

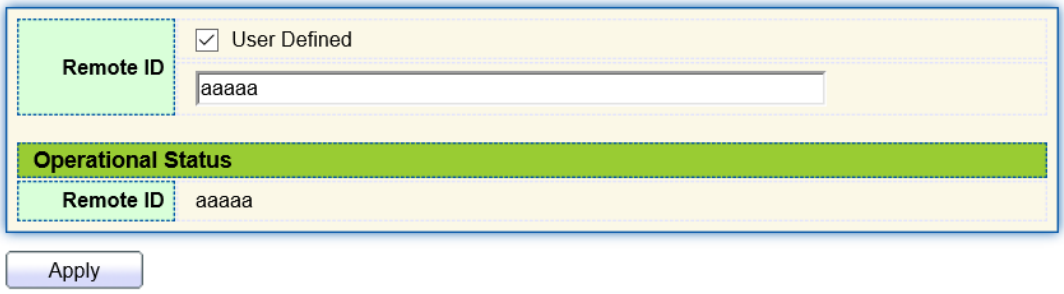
구성 항목	설명

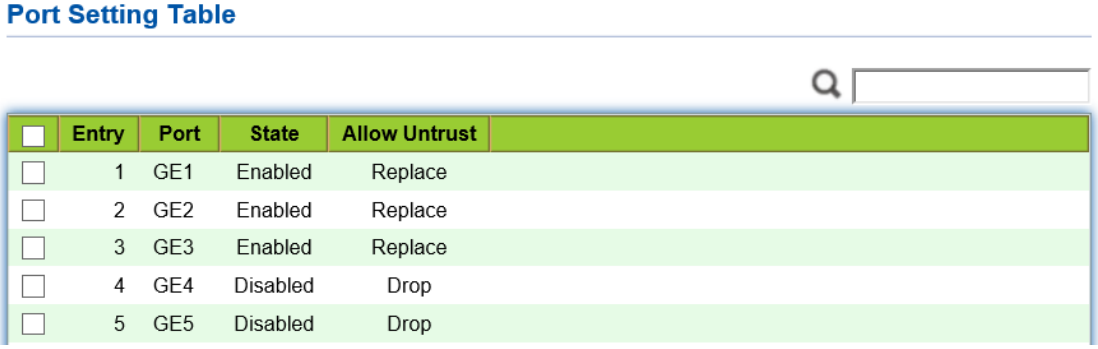
Remote ID	옵션 82 의 원격 ID 필드를 채우십시오 (예 : 사용자 정의 XXXX).
Port	옵션 82 의 포트 번호 활성화 여부
Untrust Port Access	Untrust Port는 옵션 82가 활성화 된 상태에서 메시지를 처리합니다. Maintaining : 메시지에 옵션 82 를 그대로두고 전달 Discarding : 메시지 폐기 Replacing : 회로 ID 구성에 따라 메시지의 옵션 82 필드를 교체하고 전달합니다.

Description:

옵션 82 필드는 회로 ID 또는 원격 ID 하위 옵션을 독립적으로 구성합니다.
특정 순서없이 개별적으로 또는 동시에 구성 할 수 있습니다.
사용자 표시 줄에서 DHCP 옵션 82 를 구성해야합니다. 그렇지 않으면 DHCP 서버로 전송 된 DHCP 메시지에 옵션 82 가 전달되지 않습니다.
DHCP 서버에서 DHCP 응답 메시지를 수신하면 옵션 82 가 포함 된 메시지가 필드를 삭제 한 후 전달되거나 메시지에 옵션 82 가 포함되지 않은 경우 직접 전달됩니다.

2. 각 해당 구성 항목을 입력합니다.
3. “Apply” 하고 다음과 같이 마칩니다.





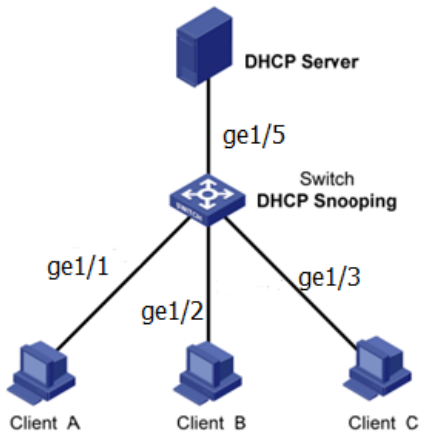
DHCP 스누핑 일반 구성의 그림

아래와 같이 스위치 포트 GE1-5는 DHCP 서버에 연결되고 포트 GE1-1, 2, 3은 DHCP

클라이언트 A, B, C 에 각각 연결됩니다.

- 스위치에서 DHCP 스누핑을 활성화합니다.
- GE1-5 를 DHCP 스누핑의 신뢰 포트로 설정합니다.
- 스위치의 옵션 82 지원 기능을 활성화합니다. 포트를 통해 흐르는 GE1-3 메시지의 경우 회로 ID 및 원격 ID 의 기본 구성에 따라 옵션 82 를 입력하십시오.

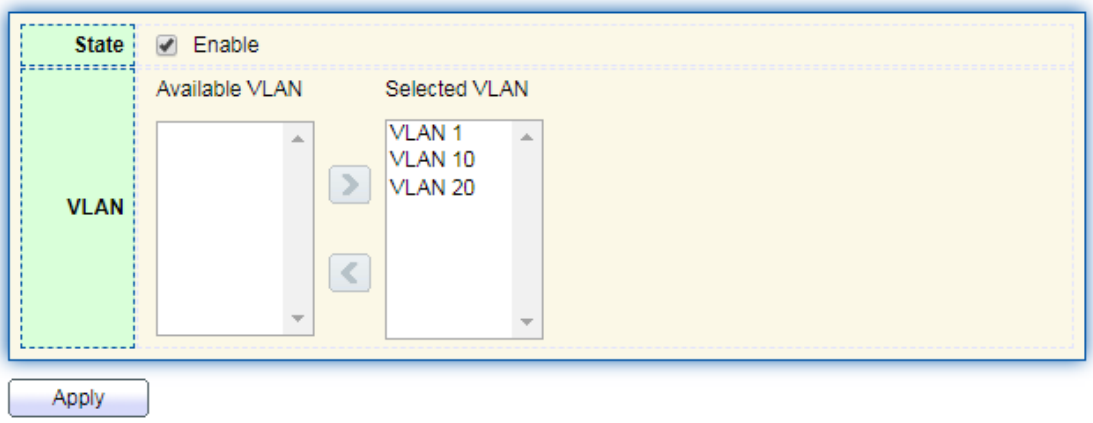
Network Diagram



Configure DHCP snooping to support Option 82

Instructions:

1. 탐색 트리에서 “Security > DHCP Snooping > Property”을 선택하여 기능을 활성화 합니다.:

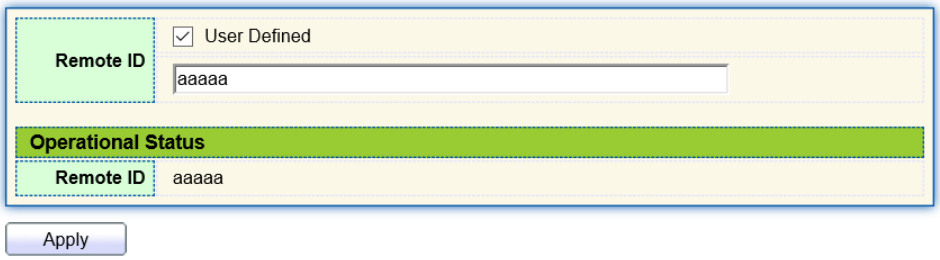


2. GE1-5 를 DHCP 스누핑의 신뢰 포트로 설정하고 해당 구성을 입력 한 후 다음과 같이 "Edit"합니다

Port Setting Table

Entry	Port	Trust	Verify Chaddr	Rate Limit
1	GE1	Enabled	Disabled	Unlimited
2	GE2	Enabled	Disabled	Unlimited
3	GE3	Enabled	Disabled	Unlimited
4	GE4	Enabled	Disabled	Unlimited
5	GE5	Enabled	Disabled	Unlimited

3. 탐색 트리에서 “Security > DHCP Snooping > Option82 Property”을 선택하고, 포트를 설정합니다. “Apply”하여 마칩니다:



Port Setting Table

Entry	Port	State	Allow Untrust
1	GE1	Disabled	Drop
2	GE2	Disabled	Drop
3	GE3	Enabled	Replace
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop

4. 옵션 82 에서 회선 ID 를 설정할 수 있도록 포트 GE3 에서 설정합니다. 탐색 트리에서 “Security > DHCP Snooping > Option82 Circuit ID” 에서 포트를 설정합니다.

Option82 Circuit ID Table

Showing All entries Showing 1 to 1 of 1 entries

Port	VLAN	Circuit ID
GE3	1	ge1/3

Add Edit Delete First Previous 1 Next Last

14.9 IP Source Guard

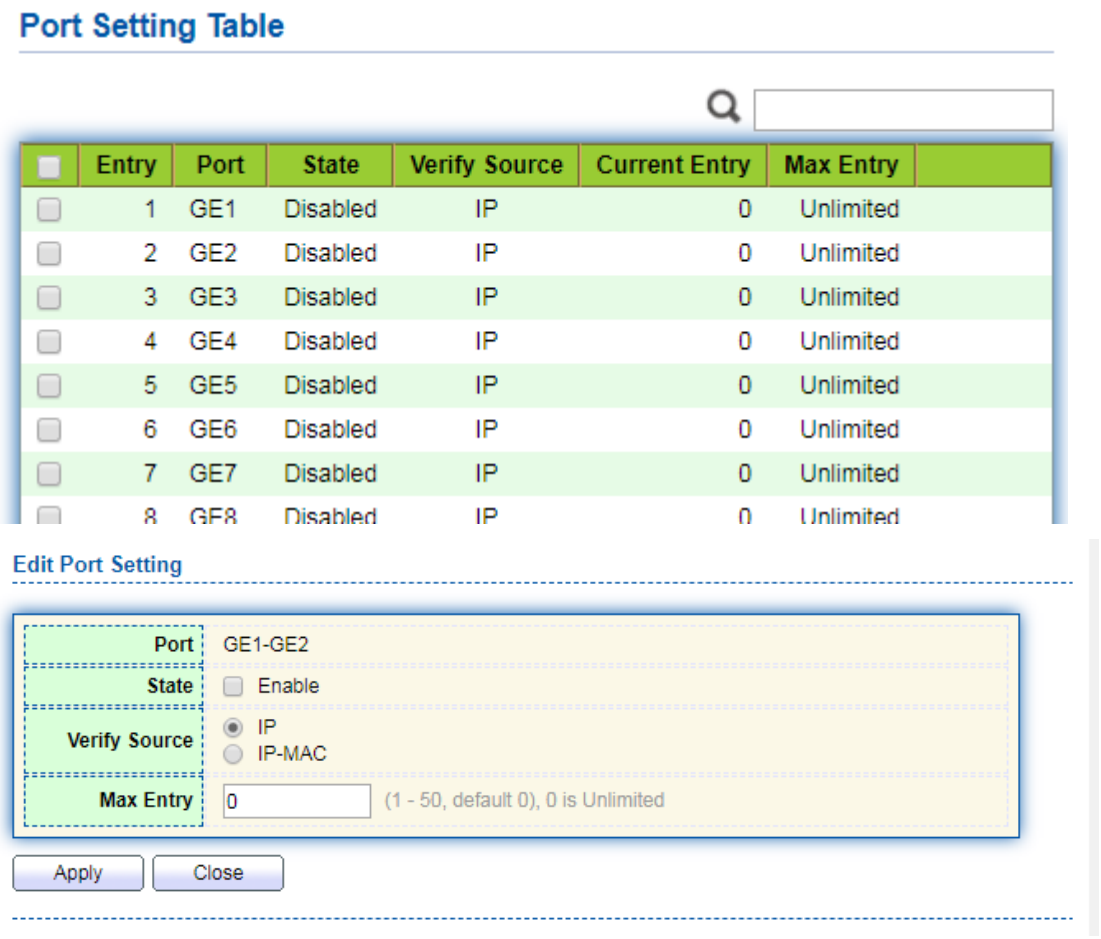
IP 소스 가드 (IPSG)는 IP / Mac 기반의 포트 트래픽 필터링 기술로 LAN 에서 IP 주소 스푸핑 공격을 방지 할 수 있습니다. IPSG 는 2 계층 네트워크에있는 터미널

장치의 IP 주소가 하이재킹되지 않도록 보장 할 수 있으며, 권한이없는 장치가 자신의 지정된 IP 주소를 통해 네트워크에 액세스하거나 네트워크를 공격하지 못하도록 할 수 있습니다.

14.9.1 Port Setting

Instructions

1. 탐색 트리에서 “Security > IP Source Guard > Port Setting”을 선택하고 포트 설정에 들어갑니다:



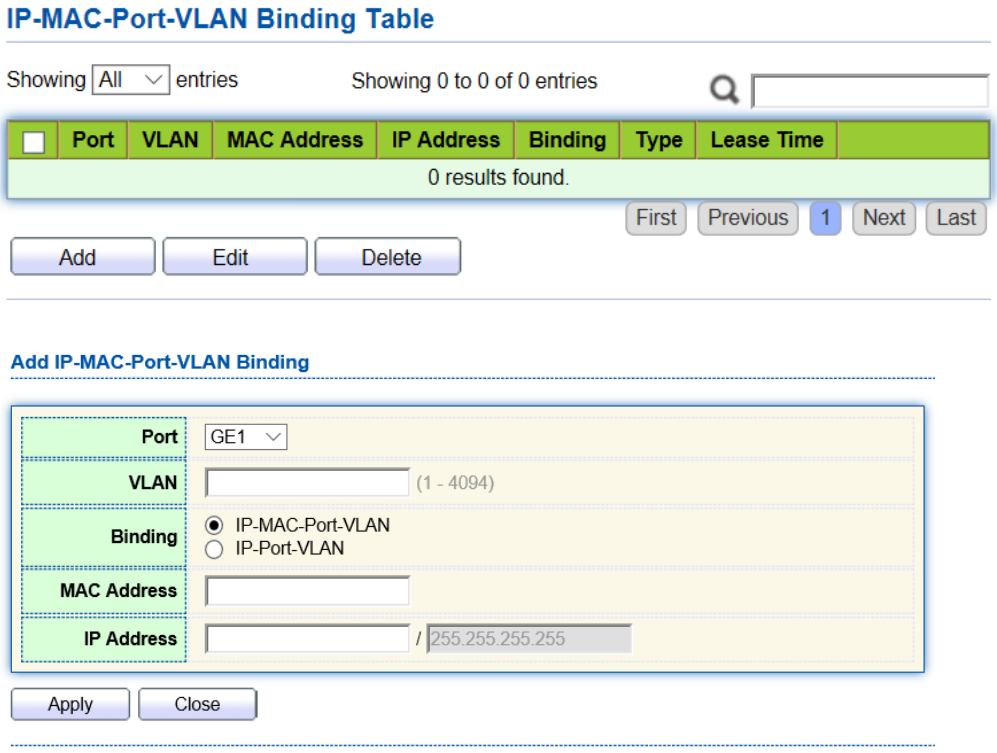
구성 항목은 다음과 같습니다.

구성 항목	설정
Port	Port 목록
State	IPSG 활성화 또는 비활성화 설정
Verify Source	기본 IP 소스 가드 필터 소스 IP 주소. "IP-MAC"는 소스 IP 주소뿐만 아니라 소스 MAC 주소도 필터링합니다.
Max Entry	허용되는 최대 포트 수

14.9.2 IMPV Binding

DHCP 네트워크에서 IP 주소를 정적으로 획득한 사용자 (DHCP 클라이언트가 아닌 사용자)는 DHCP 서버를 모방하고 DHCP 요청 메시지를 구성하는 등 네트워크를 공격 할 수 있습니다. 합법적인 DHCP 사용자가 네트워크를 사용하면 보안 위험에 노출 될 수 있습니다.
DHCP 스누핑 바인딩 테이블에서 생성된 인터페이스를 기반으로 정적 MAC 항목을 활성화하면 이러한 공격을 방지할 수 있습니다. 그런 다음 장치는 모든 DHCP 사용자에 해당하는 DHCP 스누핑 바인딩 테이블을 기반으로 명령을 자동으로 실행하여 정적 MAC 항목을 생성하고 인터페이스의 동적 항목 학습 기능을 비활성화합니다. 소스 MAC 및 정적 MAC 항목과 일치하는 메시지만 인터페이스를 통해 흐를 수 있습니다. 따라서 비 DHCP 사용자의 경우 관리자가 수동으로 구성한 정적 MAC 항목의 메시지만 통과 할 수 있고 나머지는 폐기됩니다.

Instructions:
1. 탐색 트리에서 “Security > IP Source Guard > IMPV Binding”을 선택하고, “Add”하여 새로운 IP-MAC-Port-VLAN 바인딩 그룹을 추가합니다:

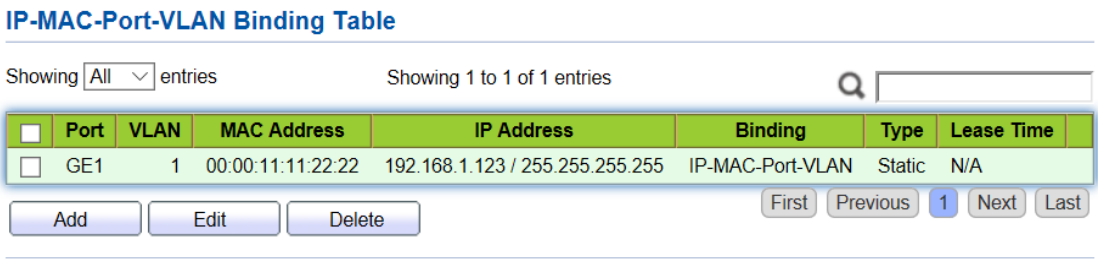


구성 항목은 다음과 같습니다.

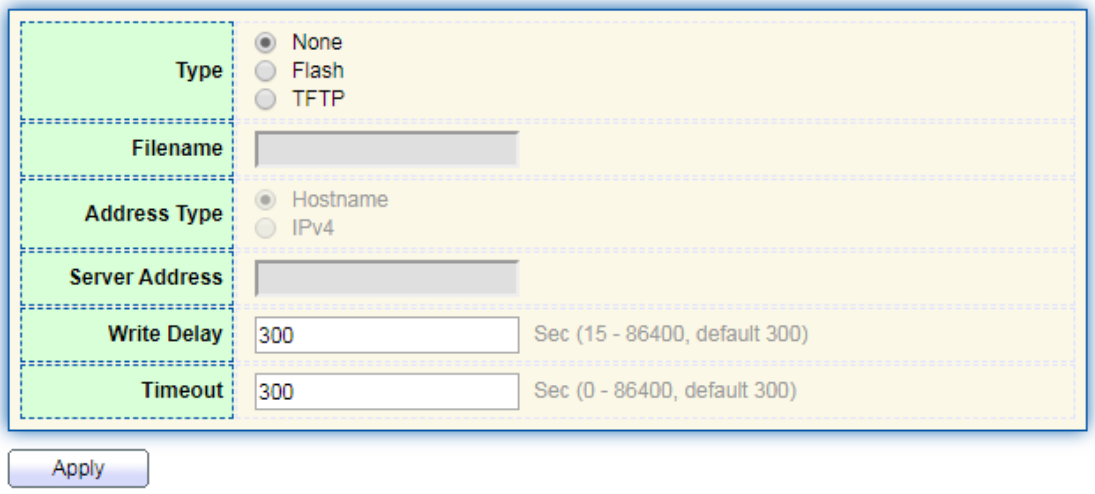
구성 항목	설명
Port	바인딩 그룹의 포트 번호
VLAN	바인딩한 VLAN ID
Binding	바인딩 설정

MAC Address	MAC address 바인딩
IP Address	IP address 바인딩

2. 해당 구성 항목을 입력합니다.
3. Apply" 하고 다음과 같이 마칩니다.



4. 탐색 트리에서 "Security > IP Source Guard > Save Database"을 선택해서 database 인터페이스에 들어갑니다:



15 ACL

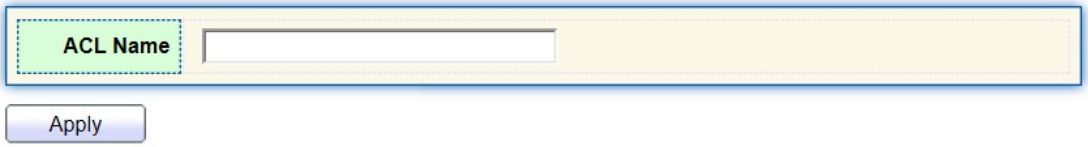
네트워크 규모 확장 및 설치 흐름은 네트워크 보안 제어 및 대역폭 할당의 위치를 강화합니다. 패킷 필터링은 불법 사용자의 액세스, 제어 흐름을 방지하고 네트워크 리소스를 절약합니다. ACL (Access Control List)은 메시지 일치 규칙 및 처리 방법을 구성하여 패킷을 필터링합니다.
메시지를 수신하는 스위치 포트는 현재 ACL 규칙에 따라 필드를 분석합니다. 특정 메시지가 식별되면 미리 정해진 정책에 따라 통과가 허용되거나 금지됩니다.

ACL 에 의해 정의 된 패킷 일치 규칙은 QoS 흐름 분류 규칙의 정의와 같이 흐름 구분이 필요한 다른 기능에서도 참조 할 수 있습니다.
ACL 은 일치 규칙 및 처리 방법을 설정하여 패킷을 필터링 할 수 있습니다. ACL 은 패킷에 적용 할 수있는 권한 및 거부 조건 모음입니다. 인터페이스가 패킷을 수신하면 스위치는 필드와 ACL 을 비교하여 지정된 표준에 따라 허용 및 거부 된 패킷을 결정합니다. ACL 은 소스 / 목적지 MAC 주소, 소스 / 목적지 IP 주소, 포트 번호 등의 일치 조건에 따라 패킷을 분류합니다. ACL 은 소스 / 목적지 주소, 포트 번호 등이 될 수있는 일치 조건에 따라 패킷을 분류합니다. ACL 은 애플리케이션 목적에 따라 다음 범주로 나눌 수 있습니다.
기본 IP ACL 은 패킷의 소스 IP 주소만을 기반으로 규칙을 구성합니다. ACL ID 범위는 100 에서 999 까지입니다. 고급 IP ACL 은 패킷의 소스 / 대상 IP 주소, IP 가 전달하는 프로토콜 유형 및 프로토콜 특성과 같은 계층 3 또는 4 정보에 따라 규칙을 준비합니다. ACL ID 의 범위는 100 ~ 999 입니다.
L2 ACL : 패킷의 소스 / 대상 MAC 주소, 802.1p 우선 순위 및 프로토콜 유형과 같은 L2 정보에 따라 규칙이 만들어집니다. ACL ID 범위는 1 ~ 99 입니다.

15.1 MAC ACL

L2 ACL: 소스 / 대상 MAC 주소, VLAN 우선 순위 및 프로토콜 유형과 같은 L2 정보에 따라 규칙이 만들어집니다.

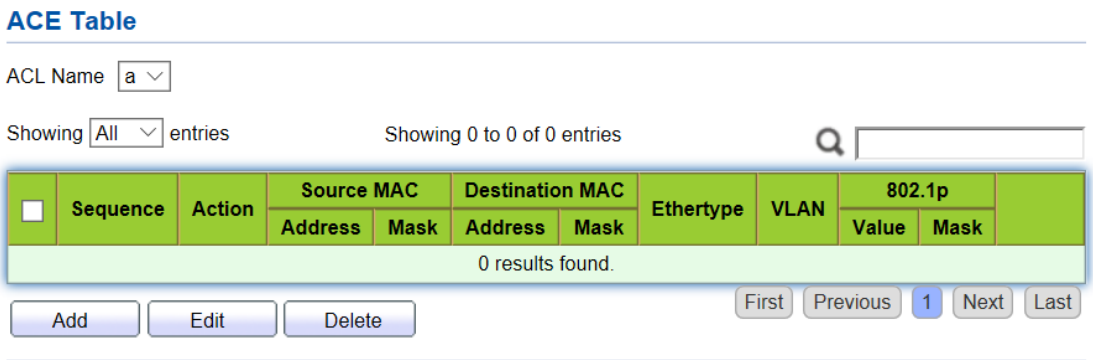
Instructions:
1. 탐색 트리에서 "ACL> MAC ACL"을 클릭합니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	MAC ACL Rules 의 이름

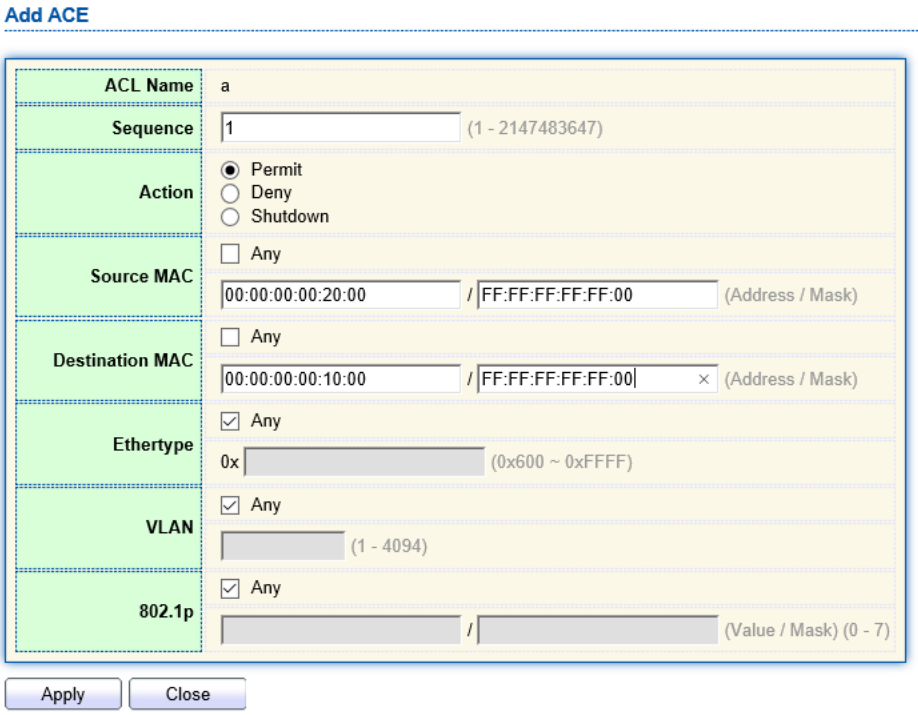
2. "ACL > MAC ACE" 을 선택하고, "Add" 하여 ACL name 을 추가합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	ACL rule 목록

3. 해당 구성 항목을 입력합니다.

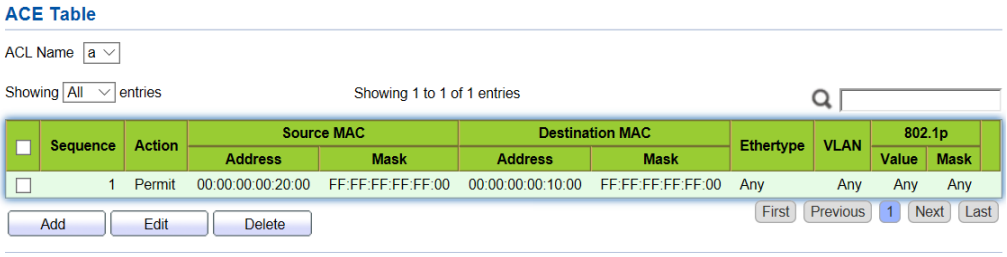


구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	ACL rule 이름
Sequence	**MAC ACL** 범위는 **1 ~ 2,147,483,647** 입니다
Action	**ACL** 동작은 "허용"또는 "거부"와 "종료"로 구분됩니다.
Source MAC	**H.H.H.H.H.H.** 형식으로 **ACL** 규칙의 소스 **MAC** 주소와 마스크를 입력합니다. **MAC** 주소를 나타내려면 **"Any"**를 선택하십시오
Destination MAC	**H.H.H.H.H.H.** 형식으로 **ACL** 규칙의 대상 **MAC** 주소와 마스크를 입력합니다. **MAC** 주소를 나타내려면 **"Any"**를 선택하십시오
EtherType	**0 x 600 ~ 0 x ffff** 범위의 이더넷 유형 **ACL** 규칙을 입력하고 **"Any"**를 선택하여 모든 유형을 나타냅니다.
VLAN	**1-4,094** 범위의 **ACL** 규칙의 **VLAN** 을 입력하고 **"Any"**를 선택하여 **VLAN** 을 나타냅니다

802.1p	**VLAN** 우선 순위와 **1 ~ 7** 범위의 **ACL** 규칙 마스크를 입력하고 **VLAN** 우선 순위를 나타내려면 **"Any"**를 선택하십시오

4. “Apply” 하고 다음과 같이 마칩니다.



15.2 IPv4 ACL

IPv4 기반 **ACL** (기본 **IP ACL)**은 패킷의 소스 **IP** 주소에 대해서만 규칙을 공식화합니다. **ACL ID** 의 범위는 **100 ~ 999** 입니다.
고급 **IP ACL** 규칙은 패킷의 소스 **/** 대상 **IP** 주소, **IP** 가 전달하는 프로토콜 유형 및 프로토콜 특성과 같은 레이어 **3** 또는 **4** 정보에 따라 만들어집니다. **ACL ID** 범위는 **100** 에서 **999** 까지입니다.

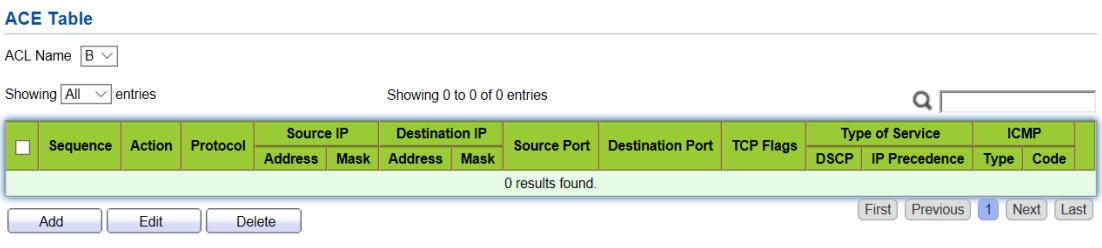
Instructions
1. 탐색 트리에서 “ACL > IPv4 ACL” 을 선택합니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	IPv4 ACL rules 이름

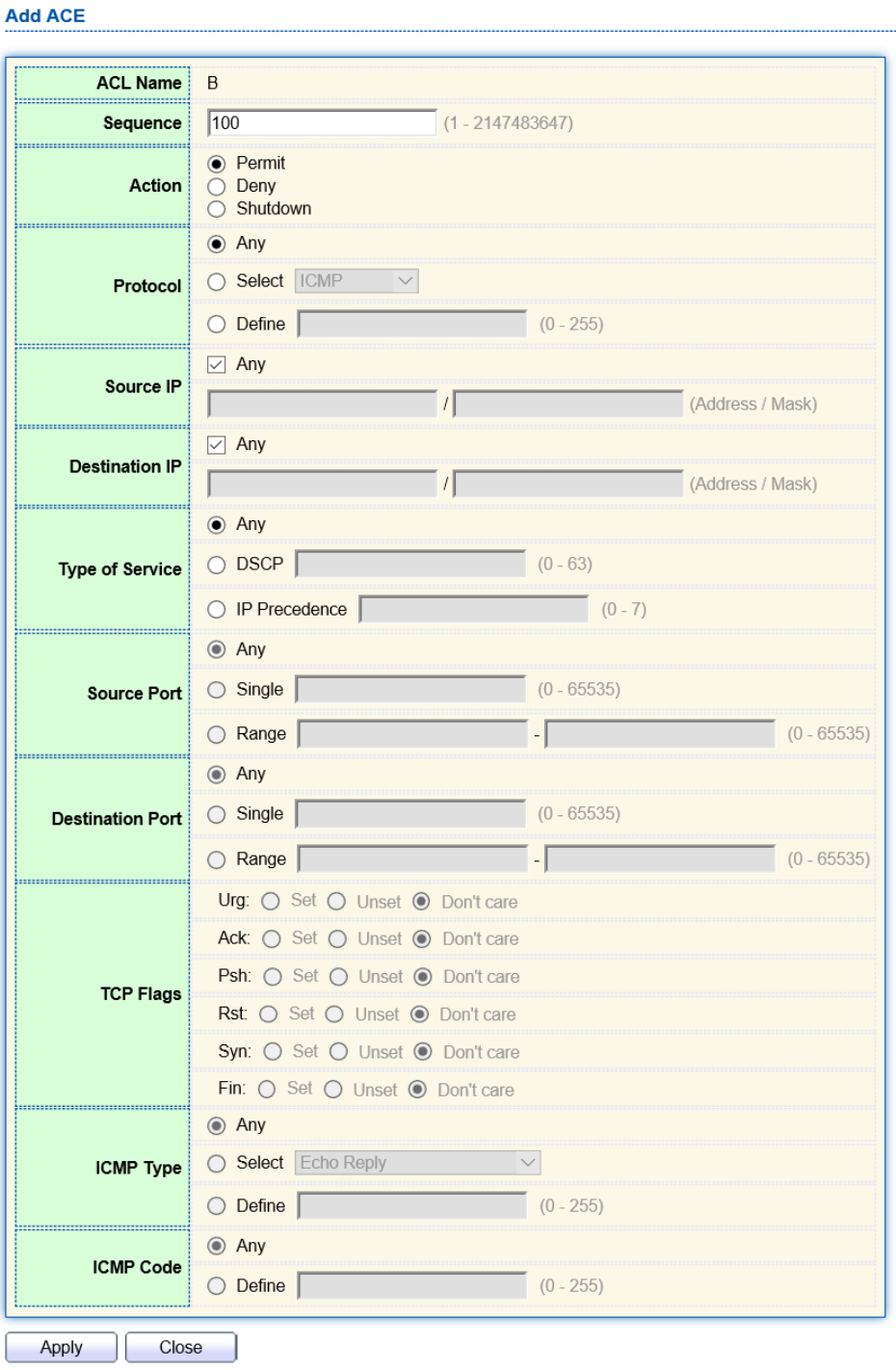
2. 탐색 트리에서 “ACL > IPv4 ACE” 을 선택하고, “Add” 하여 ACL Name 을 추가합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	ACL rule list 이름

3. Fill in corresponding 구성 항목.

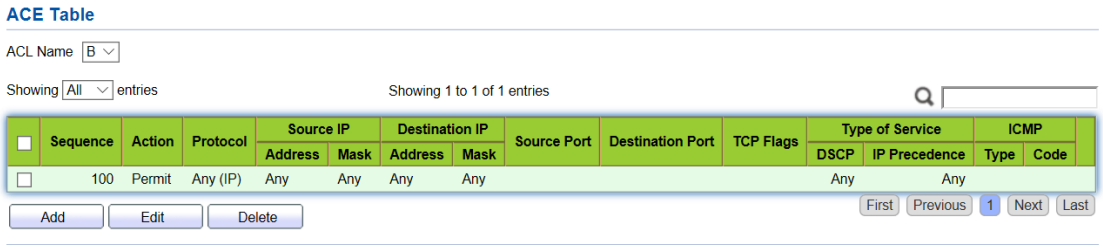


구성 항목은 다음과 같습니다.

구성 항목	설명

ACL Name	ACL rule list 이름.
Sequence	**IPv4 ACL** 의 범위는 **1 ~ 2,147,483,647** 입니다
Action	**ACL** 동작은 "허용"또는 "거부"와 "종료"로 구분됩니다.
Protocol	**ICMP, TCP** 및 **UDP** 와 같은 프로토콜 유형을 선택해야합니다. 프로토콜을 나타내려면 **"Any"**를 선택하십시오.
Source IP	**ACL** 규칙의 소스 **IP** 와 마스크를 입력합니다. 소스 **IP** 를 나타내려면 **"Any"**를 선택하십시오.
Destination IP	**ACL** 규칙의 대상 **IP** 와 마스크를 입력합니다. 대상 **IP** 를 나타내려면 **"Any"**를 선택하십시오.
Type of Service	**DSCP (0-63)** 및 **IP** 우선 순위 **(0-7)**와 같은 **ACL** 규칙의 서비스 유형을 입력합니다. 서비스 유형을 나타내려면 **"Any"**를 선택하십시오.
Source Port	단일 포트 번호 또는 범위 세그먼트 **(0-65,535)**와 같은 **ACL** 규칙의 소스 포트를 입력합니다. 소스 포트를 나타내려면 **"Any"**를 선택하십시오.
Destination Port	단일 포트 번호 또는 범위 세그먼트 **(0-65,535)**와 같은 **ACL** 규칙의 대상 포트를 입력합니다. 대상 포트를 나타내려면 **"Any"**를 선택하십시오.
TCP Flags	**URG, ACK, PSH, RST, SYN, FIN** 과 같은 **ACL** 규칙의 **TCP** 플래그를 **"Set", "Unset"**및 **"Do n't care"**와 같은 작업으로 입력합니다.
ICMP Type	**ACL** 규칙의 **ICMP** 메시지 유형을 입력합니다. **ICMP** 유형을 나타내려면 "모두"를 선택합니다.
ICMP Code	**ACL** 규칙의 **ICMP** 필드 값을 입력합니다. 필드 값을 나타내려면 "모두"를 선택합니다.

3. “Apply” 하고 다음과 같이 마칩니다.



15.3 IPv6 ACL

Instructions

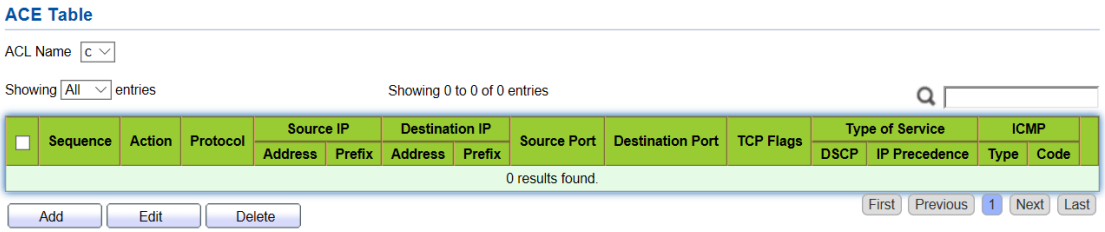
1. 탐색 트리에서 “ACL > IPv6 ACL” 을 선택합니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	IPv6 ACL rules 이름

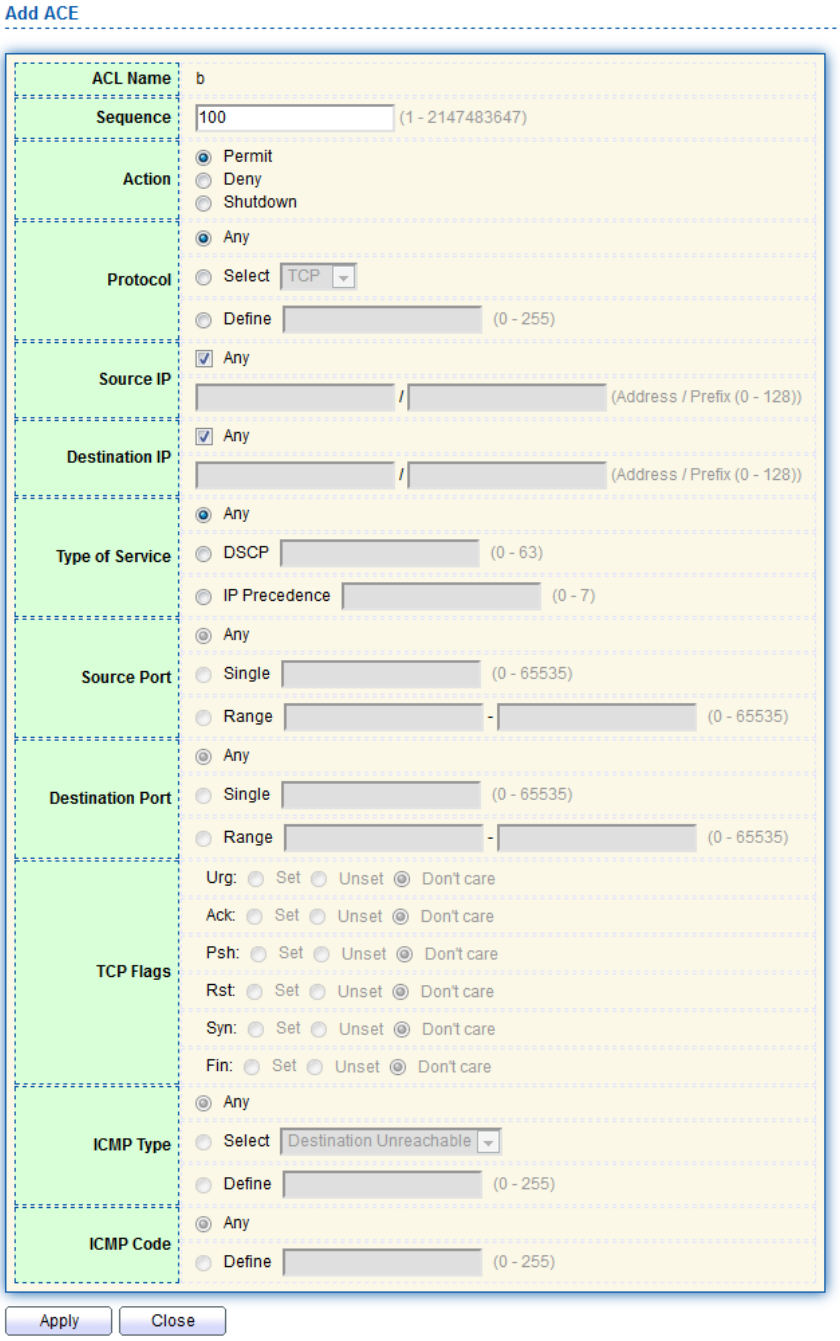
2. 탐색 트리에서 “ACL > IPv6 ACE”을 선택하고, “Add”하여 ACL Name 을 추가합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	ACL rule list 이름

3. 해당 구성 항목을 입력합니다.

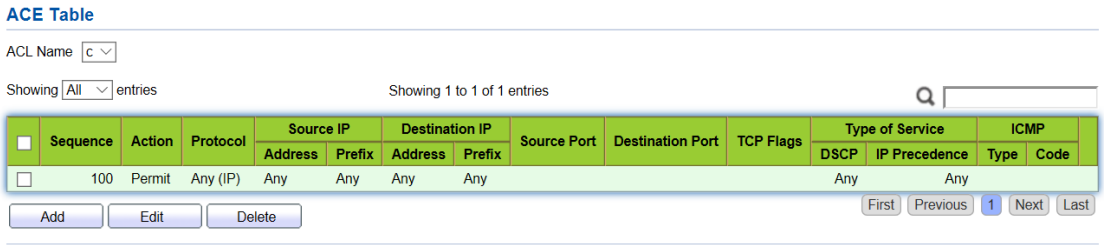


구성 항목은 다음과 같습니다.

구성 항목	설명
ACL Name	ACL rule list 이름
Sequence	**IPv6 ACL** 범위는 **1 ~ 2,147,483,647** 입니다.
Action	**ACL** 동작은 "허용"또는 "거부"와 "종료"로 구분됩니다.
Protocol	**ICMP, TCP** 및 **UDP** 와 같은 프로토콜 유형을 선택해야합니다.

	프로토콜을 나타내려면 **"Any"**를 선택하십시오.
Source IP	**ACL** 규칙의 소스 **IP** 와 마스크를 입력합니다. 소스 **IP** 를 나타내려면 **"Any"**를 선택하십시오.
Destination IP	**ACL** 규칙의 대상 **IP** 와 마스크를 입력합니다. 대상 **IP** 를 나타내려면 **"Any"**를 선택하십시오.
Type of Service	**DSCP (0-63)** 및 **IP** 우선 순위 **(0-7)**와 같은 **ACL** 규칙의 서비스 유형을 입력합니다. 서비스 유형을 나타내려면 **"Any"**를 선택하십시오.
Source Port	단일 포트 번호 또는 범위 세그먼트 **(0-65,535)**와 같은 **ACL** 규칙의 소스 포트를 입력합니다. 소스 포트를 나타내려면 **"Any"**를 선택하십시오.
Destination Port	단일 포트 번호 또는 범위 세그먼트 **(0-65,535)**와 같은 **ACL** 규칙의 대상 포트를 입력합니다. 대상 포트를 나타내려면 **"Any"**를 선택하십시오.
TCP Flags	**URG, ACK, PSH, RST, SYN, FIN** 과 같은 **ACL** 규칙의 **TCP** 플래그를 **"Set", "Unset"**및 **"Do n't care"**와 같은 작업으로 입력합니다.
ICMP Type	**ACL** 규칙의 **ICMP** 메시지 유형을 입력합니다. **ICMP** 유형을 나타내려면 "모두"를 선택합니다.
ICMP Code	**ACL** 규칙의 **ICMP** 필드 값을 입력합니다. 필드 값을 나타내려면 "모두"를 선택합니다.

4. “Apply” 하고 다음과 같이 마칩니다.

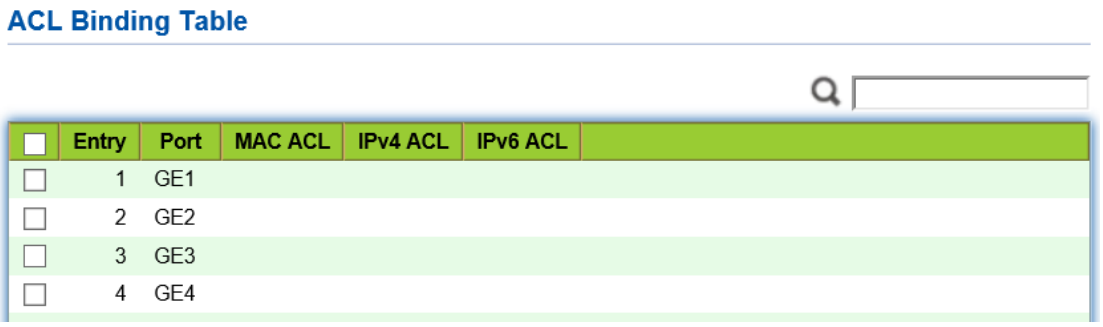


15.4 ACL Binding

목록이 생성되면 각 필수 인터페이스에 바인딩되어야합니다.

Instructions:

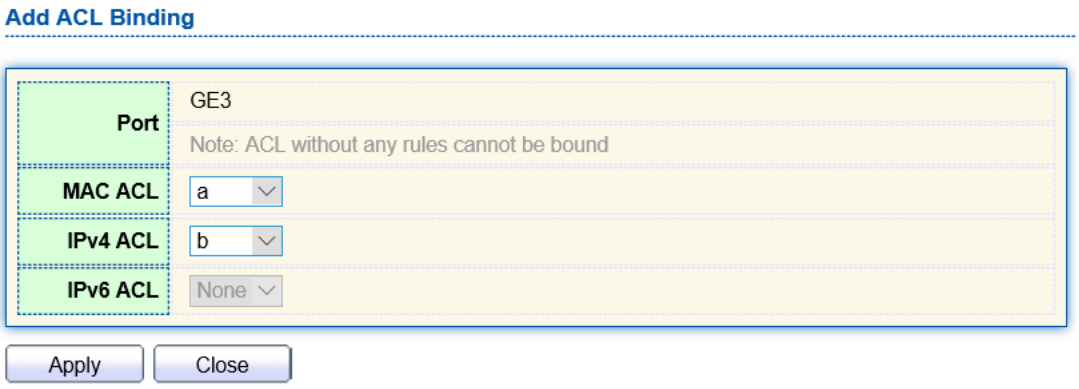
1. 다음과 같이 탐색 트리에서 “ACL > ACL Binding” 을 클릭합니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
MAC ACL	포트에 바인딩 된 **MAC ACL** 이름
IPv4 ACL	포트에 바인딩 된 **IPv4 ACL** 이름 **(IPv6 ACL** 과 상호 배타적**)**
IPv6 ACL	포트에 바인딩 된 **IPv6 ACL** 이름 **(IPv4 ACL** 과 상호 배타적**)**

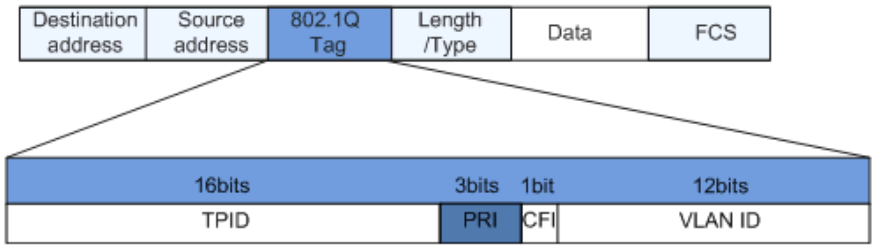
2. 해당 구성 항목을 입력합니다.
3. “Apply” 하고 다음과 같이 마칩니다.



16 QoS

QoS (Quality of Service)는 고객의 요구 사항을 충족하는 서비스 제공 업체의 능력과 인터넷을 통해 패킷을 전송하는 능력을 평가합니다. 다양한 측면에 따라 다양한 서비스를 평가할 수 있습니다. **QoS**는 일반적으로 대역폭, 지연, 지연 변동 및 전달 중 패킷 손실률과 같은 핵심 요구 사항을 지원하는 서비스 기능의 평가를 나타냅니다.
처리량이라고도하는 대역폭은 **Kbit / s** 단위로 지정된 시간 동안 비즈니스 흐름의 평균 속도를 나타냅니다. 지연은 네트워크를 통한 비즈니스 흐름에 필요한 평균 시간을 나타냅니다. 네트워크 장치의 경우 일반적인 지연 요구 사항은 다음과

같습니다.
두 가지 지연 수준이 있습니다. 즉, 우선 순위가 높은 비즈니스는 우선 순위 대기열의 스케줄링 방법을 통해 가능한 한 빨리 서비스를 제공 할 수 있고, 낮은 우선 순위 비즈니스는 그 후에 서비스를 받습니다.
지연 변동은 네트워크를 통해 흐르는 비즈니스의 시간 변화를 나타냅니다.
패킷 손실률은 전송 중 손실 된 비즈니스 흐름의 비율을 나타냅니다.
최신 전송 시스템은 매우 안정적이므로 네트워크 정체로 인해 정보가 손실되는 경우가 많습니다. 대기열 오버플로로 인한 패킷 손실이 가장 일반적인 상황입니다
기존 **IP** 네트워크의 모든 메시지는 동일하게 취급됩니다. 모든 네트워크 장치는 **FIFO** 기반으로 메시지를 처리하고 안정성, 전송 지연 또는 기타 성능을 보장하지 않고 대상으로 메시지를 전송하기 위해 모든 노력을 기울입니다.
빠르게 변화하는 **IP** 네트워크에서 새로운 애플리케이션이 계속 등장함에 따라 네트워크 서비스 품질이 지속적으로 향상됩니다. 예를 들어 **VoIP**, 비디오 및 기타 지연에 민감한 서비스는 메시지 전송 지연에 대해 더 높은 표준을 설정했습니다. 단기간 메시지 전송이 일반적인 추세였습니다. 요구 사항이 다른 음성, 비디오 및 데이터 서비스를 지원하기 위해 네트워크는 비즈니스 유형을 식별하고 해당 서비스를 제공해야합니다.
비즈니스 유형을 구별하는 기능은 해당 서비스를 제공하기위한 전제 조건이므로 기존의 최선형 서비스는 더 이상 애플리케이션 요구 사항을 충족하지 못합니다. 따라서 **QoS** 가 등장합니다. 네트워크 정체를 방지 및 처리하고 패킷 손실률을 줄이기 위해 네트워크 흐름을 조절합니다. 한편, 사용자는 전용 대역폭을 즐길 수 있고 비즈니스는 서비스 품질을 향상시켜 네트워크 서비스 용량을 완벽하게 할 수 있습니다.
QoS 우선 순위는 메시지 유형에 따라 다릅니다. 예를 들어, **VLAN** 메시지는 **CoS (Class of Service)** 필드라고도하는 **802.1p** 를 사용하는 반면 **IP** 메시지는 **DSCP** 를 사용합니다. 우선 순위를 유지하려면 메시지가 네트워크를 통해 흐를 때 다양한 네트워크에 연결된 게이트웨이에서 이러한 필드를 매핑해야합니다.
VLAN 프레임 헤더의 **802.1p** 우선 순위
일반적으로 **VLAN** 프레임은 레이어 **2** 장치간에 상호 작용합니다. **VLAN** 프레임 헤더의 **PRI** 필드 (즉, **802.1p** 우선 순위) 또는 **CoS** 필드는 **IEEE 802.1Q** 의 정의에 따라 서비스 품질 요구 사항을 식별합니다.



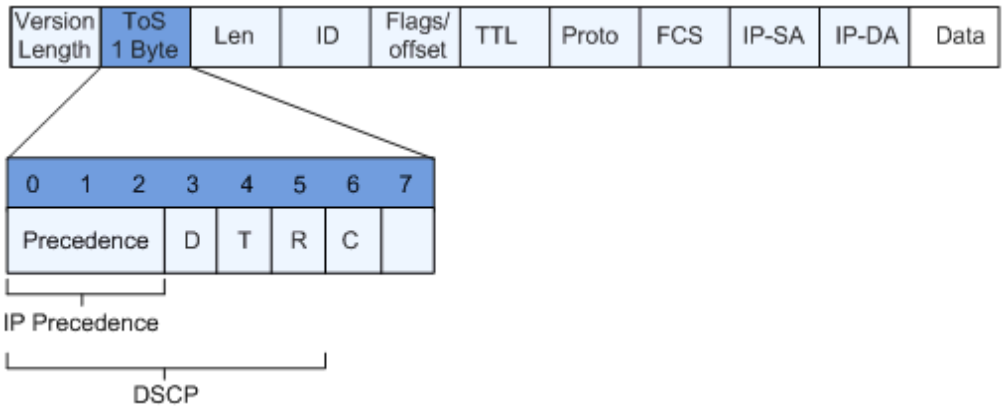
< VLAN 프레임의 802.1p 우선 순위>

802.1Q 헤더에는 3 비트 PRI 필드가 있습니다. PRI 필드는 높음에서 낮음까지

7 에서 0 까지의 8 CoS 비즈니스 우선 순위를 정의합니다.

IP 우선 순위 / DSCP 필드

RFC791 정의에 따르면 IP 메시지 헤더의 ToS (Type of Service) 도메인은 8 비트로 구성됩니다. 이 중 3 비트 long Precedence 필드는 다음과 같이 IP 메시지 우선 순위를 식별합니다



0 ~ 2 비트는 **7 ~ 0** 범위의 메시지 전송 우선 순위를 나타내는 우선 순위 필드이며, 네트워크 제어 통신을 라우팅하거나 업데이트하기 위해 일반적으로 예약 된 최고 우선 순위는 레벨 **7** 또는 **6** 입니다. 사용자 수준 응용 프로그램은 수준 **0 ~ 5** 에만 액세스 할 수 있습니다.

ToS 도메인은 **Precedence** 필드 외에 **D, T** 및 **R** 비트도 포함합니다. **D-** 비트는 지연 요구 사항을 나타냅니다 (일반 지연의 경우 **0,** 낮은 지연의 경우 **1). T** 비트는 처리량을 나타냅니다 (일반 처리량의 경우 **0,** 높은 처리량의 경우 **1). R** 비트는 신뢰성을 나타냅니다 (일반 신뢰성의 경우 **0,** 높은 신뢰성의 경우 **1). ToS** 도메인은 **6** 비트와 **7** 비트를 예약합니다.

RFC1349 는 통화 비용을 나타내는 **C** 비트를 추가하여 **ToS** 도메인을 재정의합니다. **IETF DiffServ** 그룹은 **RFC2474** 의 **IPv4** 메시지 헤더에있는 **ToS** 도메인의 **0 ~ 5** 비트를 **DSCP** 로 재정의하고 위 그림과 같이 **DS (Differentiated Service)** 바이트로 이름을 바꿉니다.

DS 필드의 처음 **6** 비트 **(0-5** 비트)는 **DSCP (DS** 코드 포인트)를 구분하며 상위 **2** 비트 **(6-7** 비트)는 예약됩니다. 하위 **3** 비트 **(0-2** 비트)는 **CSCP (Class Selector Code Point)**이며 동일한 **CSCP** 값은 동일한 클래스의 **DSCP** 를 나타냅니다. **DS** 노드는 **DSCP** 값에 따라 해당 **PHB (**홉당 동작)를 선택합니다.

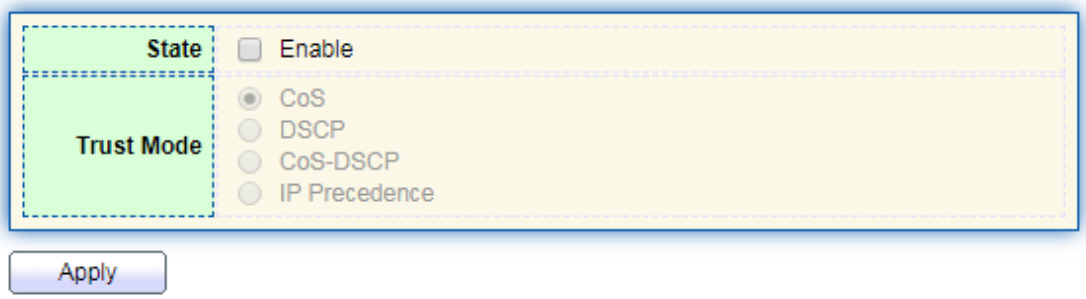
16.1 General

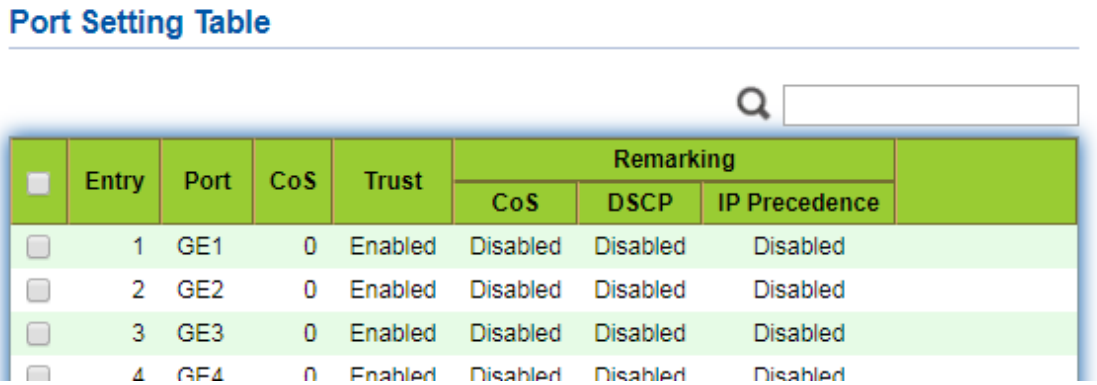
16.1.1 Property

동시에 메시지 간의 리소스 사용 권한 경쟁으로 인한 네트워크 혼잡은 일반적으로 큐 스케줄링을 통해 해결되므로 간헐적 인 혼잡을 피할 수 있습니다. 대기열 스케줄링 기술에는 **SP (Strict-Priority), WFQ (Weighted Fair Queue), WRR (Weighted Round Robin)** 및 **DRR (Deficit Round Robin, RR** 기술에서도 확장 됨)이 포함됩니다.

글로벌 및 포트 스케줄링 설정에 대한 방법:

1. 탐색 트리에서 "QoS > General > Property" 을 선택합니다.





구성 항목은 다음과 같습니다.

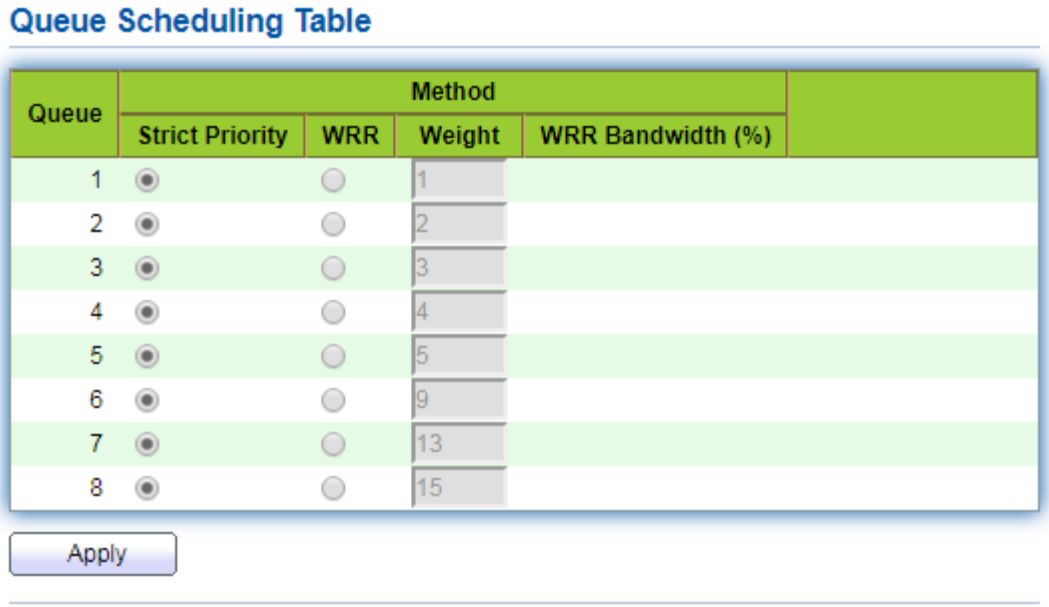
구성 항목	설명
State	글로벌 **QoS** 기능 전환
Trust Mode	**CoS, DSCP, CoS-DSCP** 및 **IP** 우선 순위로 나눌 수 있습니다

Port Setting Table 의 구성 항목은 다음과 같습니다.

구성 항목	설명
CoS	**0** 에서 **7** 까지
Port Trust Mode	포트 **QoS** 기능 전환
CoS	**CoS** 필드 표시
DSCP	**DSCP** 필드 표시
IP Priority	**IP Priority** 필드를 표시

16.1.2 Queue Scheduling

1. 탐색 트리에서 "QoS > General > Queue Scheduling"을 선택하고, "Apply"하여 완료합니다.

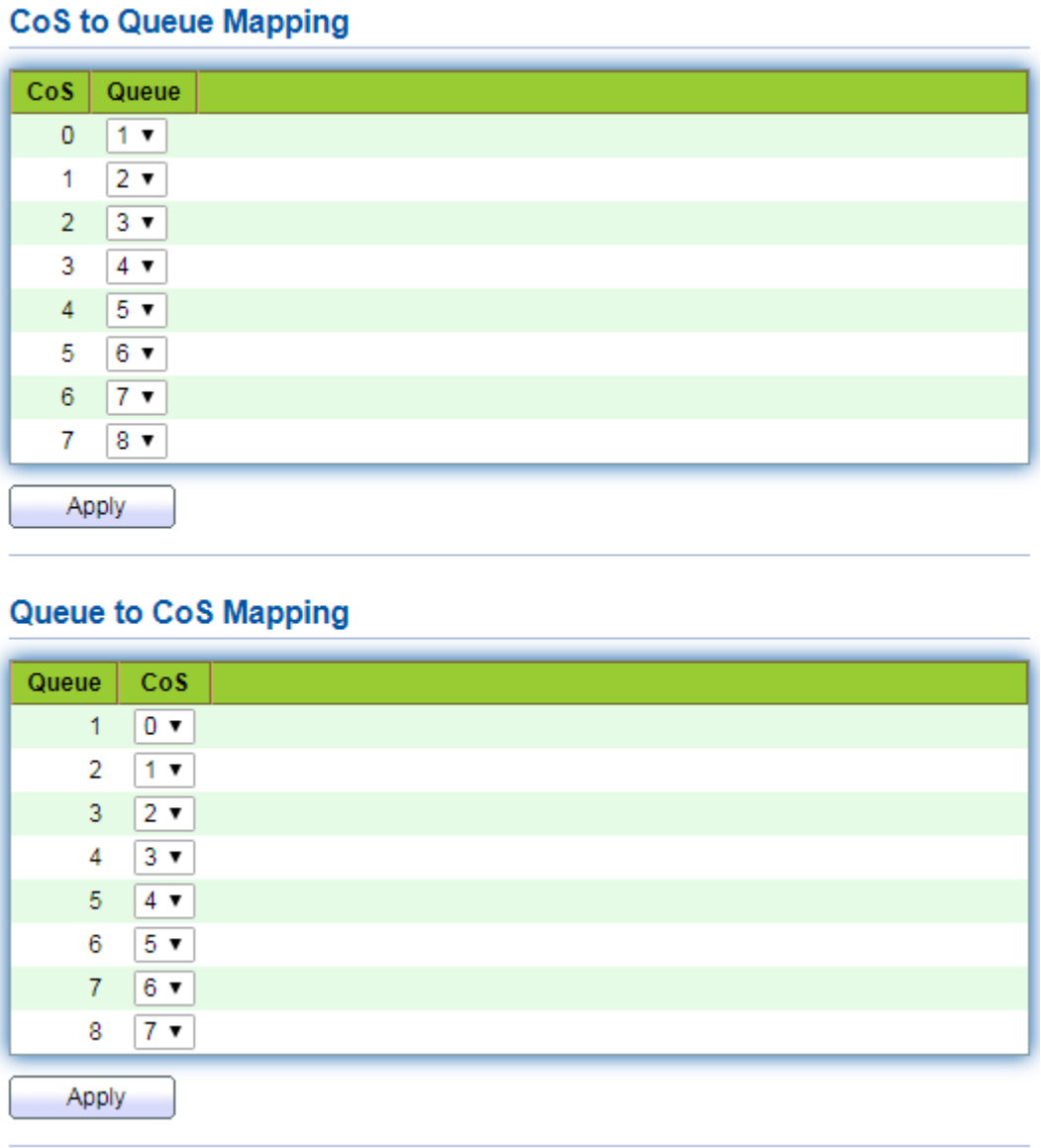


구성 항목은 다음과 같습니다.

구성 항목	설명
Strict Priority	SP mode
WRR	WRR mode
Weight	대기열이 차지하는 **WRR** 의 대역폭 비율

16.1.3 CoS Mapping

1. 탐색 트리에서 “QoS > General > CoS Mapping” 을 선택하고, “Apply” 하여 마칩니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
CoS	802.1p priority
Queue	포트 큐

16.1.4 DSCP Mapping

1. “QoS > General > DSCP Mapping”을 선택하고, “Apply”하여 마칩니다.

DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1	16 [CS2]	3	32 [CS4]	5	48 [CS6]	7
1	1	17	3	33	5	49	7
2	1	18 [AF21]	3	34 [AF41]	5	50	7
3	1	19	3	35	5	51	7
4	1	20 [AF22]	3	36 [AF42]	5	52	7
5	1	21	3	37	5	53	7
6	1	22 [AF23]	3	38 [AF43]	5	54	7
7	1	23	3	39	5	55	7
8 [CS1]	2	24 [CS3]	4	40 [CS5]	6	56 [CS7]	8
9	2	25	4	41	6	57	8
10 [AF11]	2	26 [AF31]	4	42	6	58	8
11	2	27	4	43	6	59	8
12 [AF12]	2	28 [AF32]	4	44	6	60	8
13	2	29	4	45	6	61	8
14 [AF13]	2	30 [AF33]	4	46 [EF]	6	62	8
15	2	31	4	47	6	63	8

Apply

Queue to DSCP Mapping

Queue	DSCP
1	0 [CS0]
2	8 [CS1]
3	16 [CS2]
4	24 [CS3]
5	32 [CS4]
6	40 [CS5]
7	48 [CS6]
8	56 [CS7]

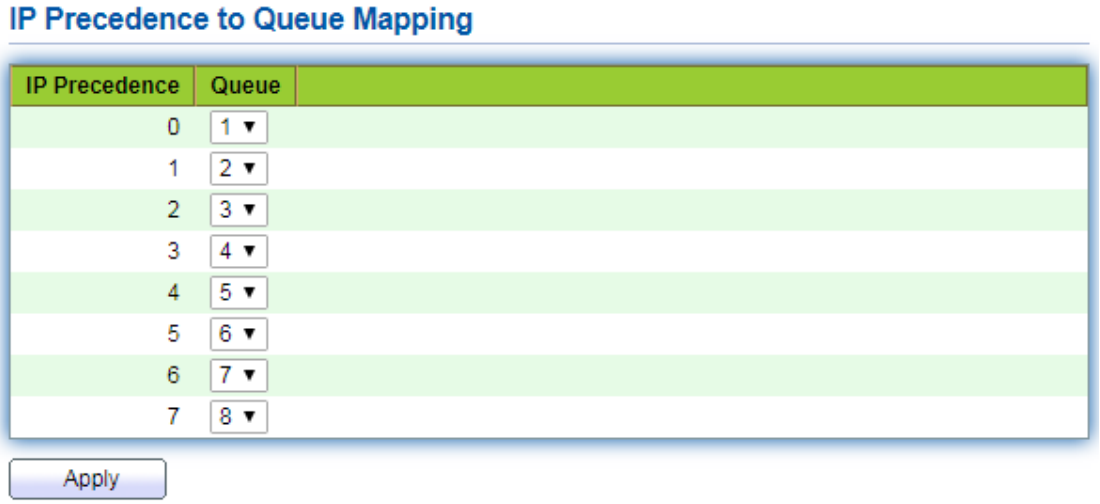
Apply

구성 항목은 다음과 같습니다.

구성 항목	설명
DSCP	IP DHCP domain priority
Queue	Port queue

16.1.5 IP Precedence Mapping

1. 탐색 트리에서 “QoS > General > IP Precedence Mapping”을 선택하고, 이 페이지에서 “Apply”하여 마칩니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
IP Precedence	IP TOS domain priority
Queue	Port queue

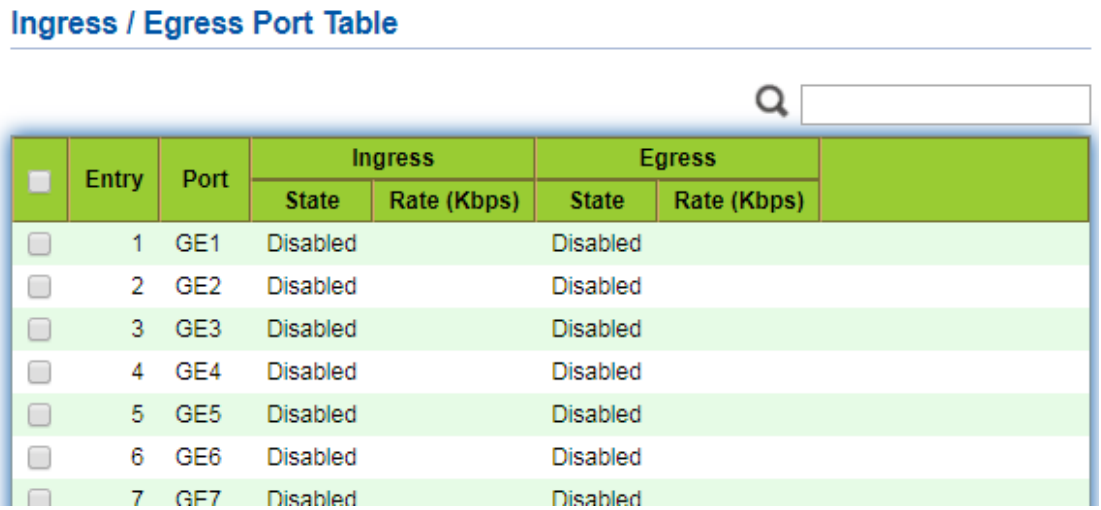
16.2 Rate limit

16.2.1 Ingress / Egress Port

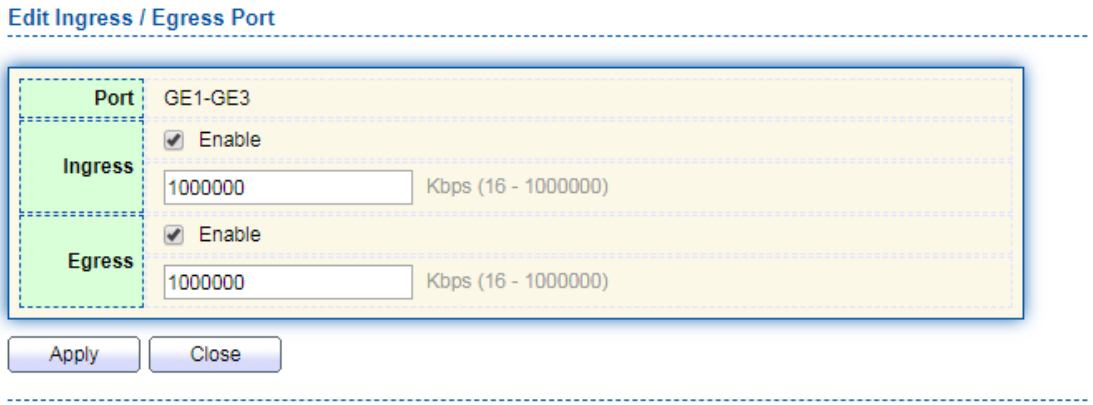
물리적 인터페이스에서 데이터 송수신에 대한 속도 제한을 나타냅니다.
흐름을 전송하기 전에 송신에서 속도 제한을 제한하여 모든 송신 메시지 흐름을 제어합니다.
흐름을 받기 전에 수신에서 속도 제한을 제한하여 모든 수신 메시지 흐름을 제어합니다.

Instructions:

1. 탐색 트리에서 “QoS > Rate Limit > Ingress / Egress Port” 을 선택하여 rate-limiting port 를 선택합니다:



2. 속도 제한을 위한 포트를 선택하고 하단에서 "Edit"하여 기능을 전환하고 속도를 지정합니다. 다음과 같이 "Apply"하고 완료합니다:



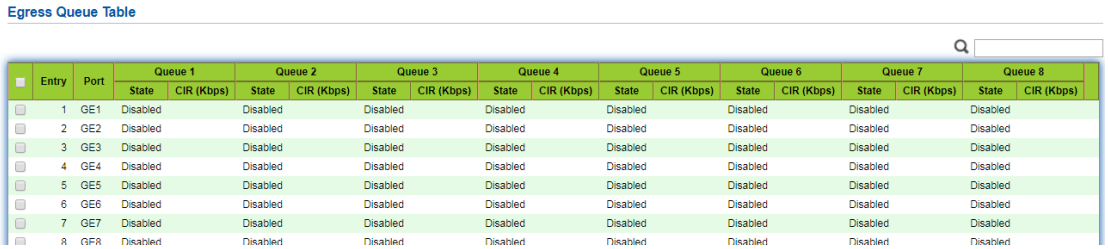
구성 항목은 다음과 같습니다.

구성 항목		설명
Ingress	Enabled	활성화 여부
	Rate	범위(16 to 1,000,000 Kbps)
Egress	Enabled	활성화 여부
	Rate	범위(16 to 1,000,000 Kbps)

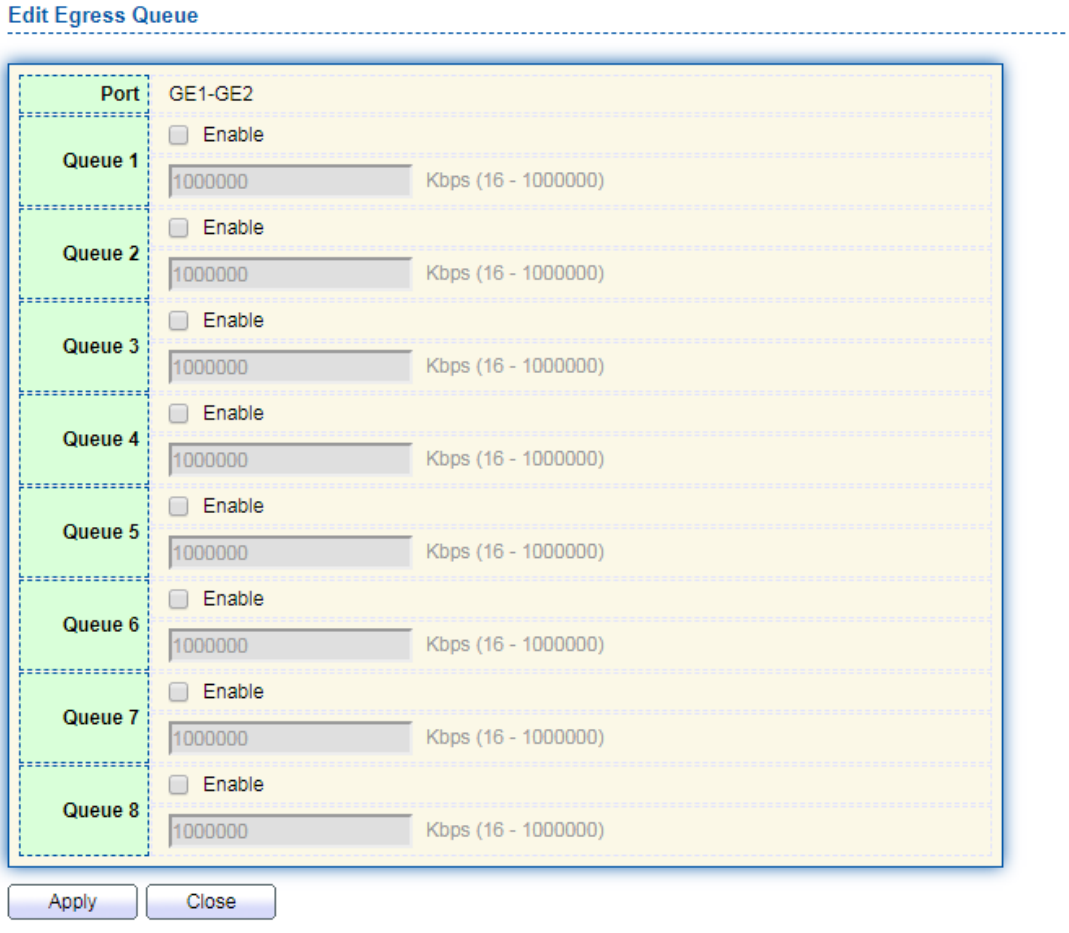
16.2.2 Egress Queue

egress queue 설정 방법

1. 탐색 트리에서 “QoS > Rate Limit > Egress Queue”을 선택합니다.



2. 포트를 선택하고, “Edit”하여 포트 설정에 들어갑니다.



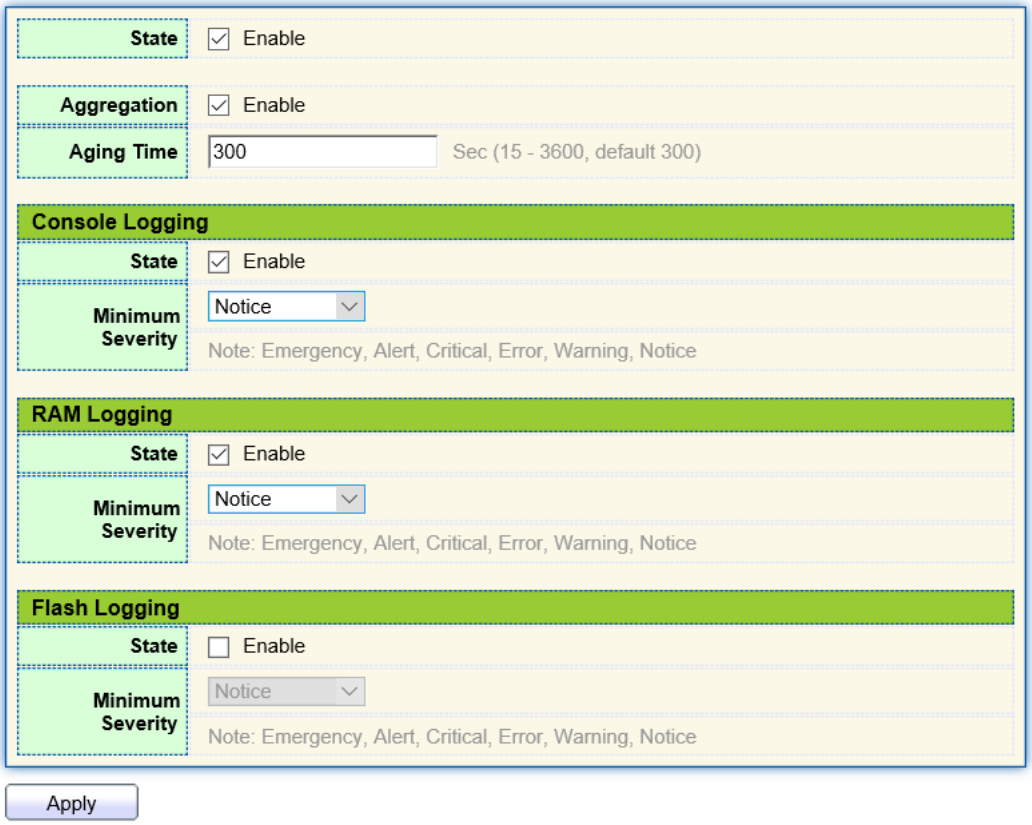
17 Diagnostics

17.1 Logging

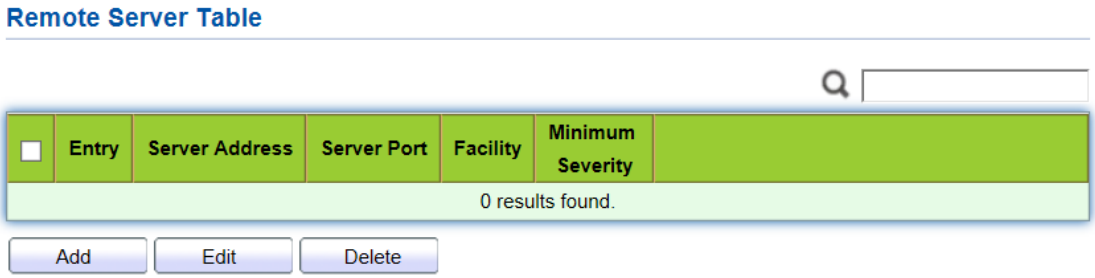
log, info integration, aging time and configuration level 을 설정합니다. 스위치의 작업 로그를 TFTP 서버에 업로드합니다.

Instructions:

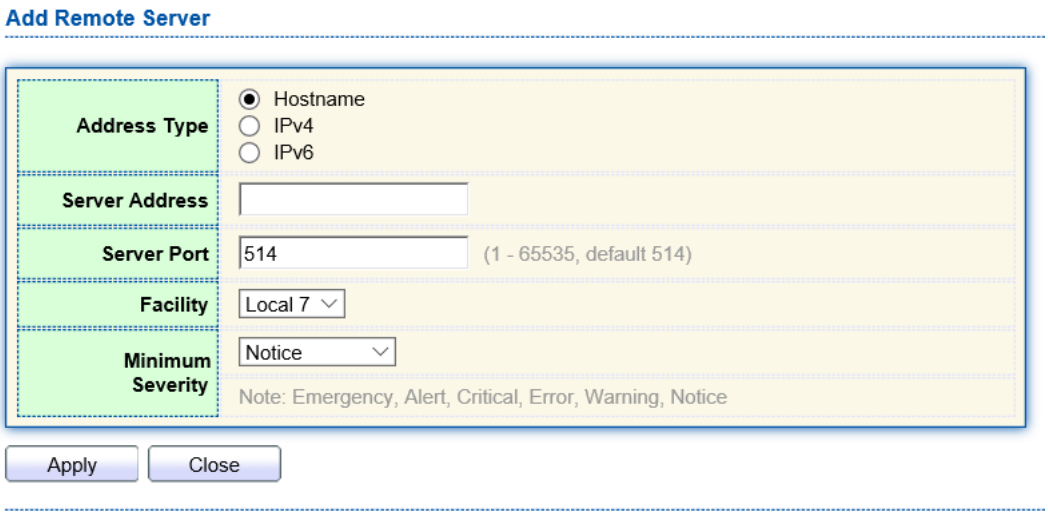
1. 탐색 트리에서 “Diagnostics > Logging > Property”에서 로그를 활성화/비활성화하고, 송신 터미널을 선택하고, 심각도 수준을 구성하는 등의 작업을 다음과 같이 수행합니다.:



2. 탐색 트리에서 “Diagnostics > Logging > Remote Server”을 선택하여 서버 설정을 추가하거나 확인합니다:



3. “Add”하여 새 리모트 로그 서버를 설정하고, 구성된 서버를 “Edit”합니다. “Apply”하여 작업을 완료합니다:

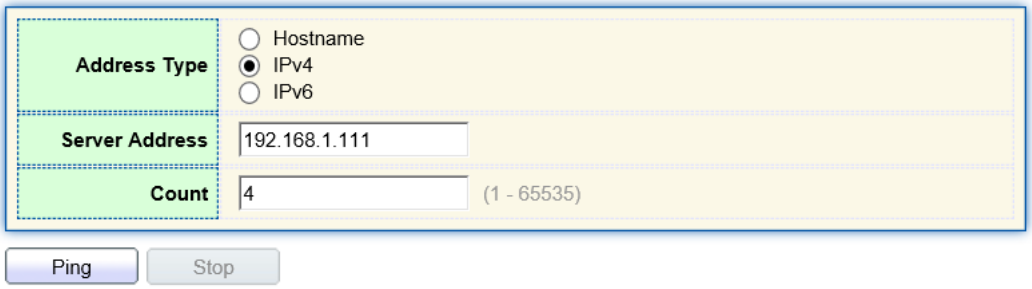


17.2 Ping

Ping 명령은 지정된 IP 주소 및 호스트 이름의 가용성을 확인하고 그에 따라 통계를 전송합니다.

Instructions:

1. 탐색 트리에서 “Diagnostics > Ping”을 선택하고, Ping Test 할 정보를 입력합니다:



2. “Ping”을 클릭해서 패킷 전송 테스트를 진행하고 결과를 확인합니다:

Ping Result

Packet Status	
Status	Success.
Transmit Packet	4
Receive Packet	4
Packet Lost	0 %

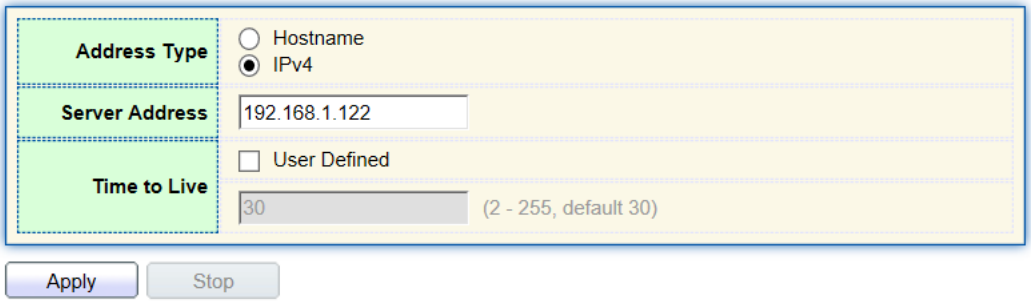
Round Trip Time	
Min	0 ms
Max	0 ms
Average	0 ms

17.3 Traceroute

Traceroute 는 작은 패킷을 전송 한 후 대상 장치에서 다시 수신 할 때까지의 기간을 측정합니다.

Instructions:

1. 탐색 트리에서 “Diagnostics > Traceroute”을 선택하고 테스트할 정보를 입력합니다:



2. “Apply”하여 테스트를 시작하고, 결과를 확인합니다:

Traceroute Result

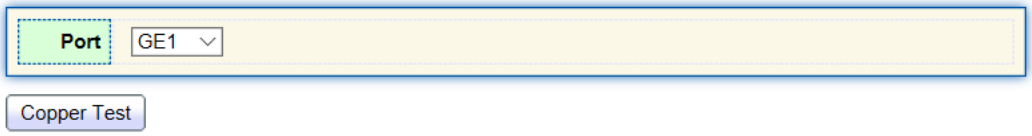
```
traceroute to 192.168.1.122 (192.168.1.122), 30 hops max, 38 byte packets
 1  192.168.1.122 (192.168.1.122)  0.000 ms  0.000 ms  0.000 ms
```

17.4 Copper Test

Copper test 는 유입 케이블 상태를 평가하고 반사 된 전압 강도에 따라 결함(오류로 약 5m)을 찾습니다.

Instructions:

1. 탐색 트리에서 “Diagnostics > Copper Test” 을 선택하고, 테스트를 할 포트를 지정합니다:



Copper Test

2. “Copper Test”를 클릭하고, 결과를 확인합니다.

Copper Test Result

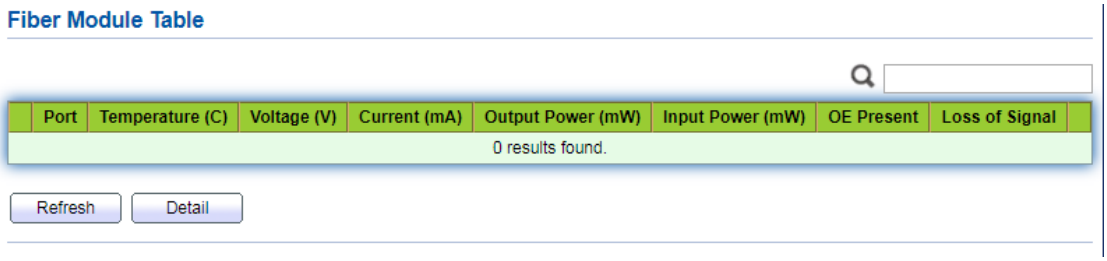
Cable Status	
Port	GE1
Result	Open Cable
Length	2.92 M

17.5 Fiber Module

광모듈의 DDM 정보를 확인합니다.

Instructions:

1. 탐색 트리에서 “Diagnostics > Fiber Module”을 선택합니다:



Note:

- 광모듈 정보는 해당 인터페이스 상태가 UP 인 경우에만 확인할 수 있습니다.

17.6 UDLD

UDLD (Unidirectional Link Detection) : 광섬유 또는 트위스트 페어로 연결된 이더넷 링크의 물리적 구성을 모니터링하는 데 사용되는 Cisco 프라이빗 레이어 2 프로토콜입니다. 단방향 링크가 나타나면(예 : 사용자에게 데이터를 보낼 수 있고 수신 할 수도 있지만 사용자가 보낸 데이터를 받을 수 없는 상태), UDLD 는 이 상황을 감지하고, 해당 인터페이스를 닫고 경고 메시지를 보냅니다. 단방향 링크는 많은 문제, 특히 스패닝 트리를 유발하여 루프백을 일으킬 수 있습니다.

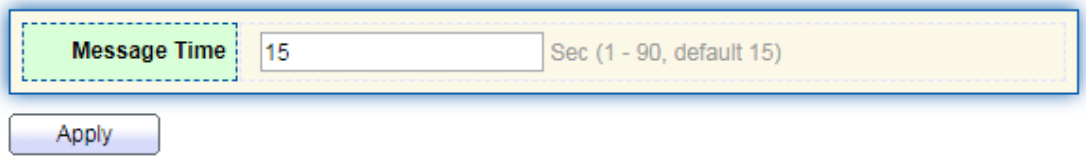
참고 : UDLD 가 정상적으로 실행되려면 링크의 양쪽 끝에서 장치가 지원해야합니다.

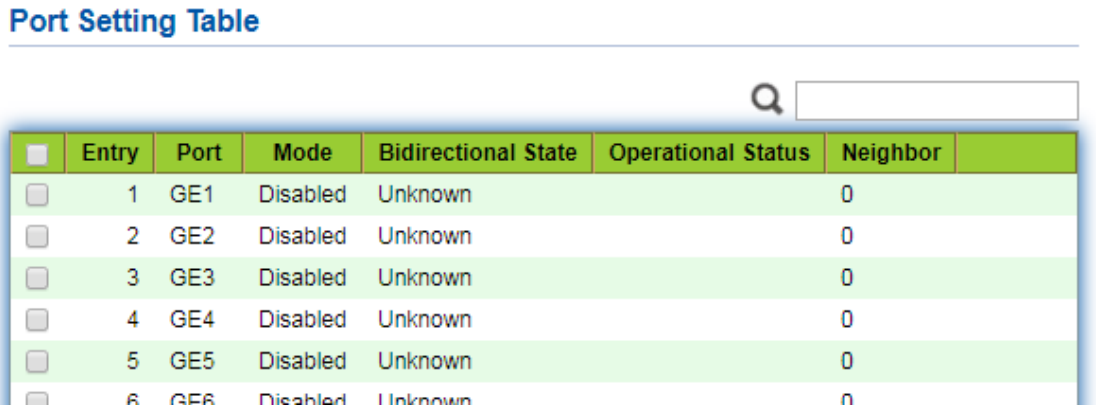
17.6.1 Property

글로벌 및 포트 설정

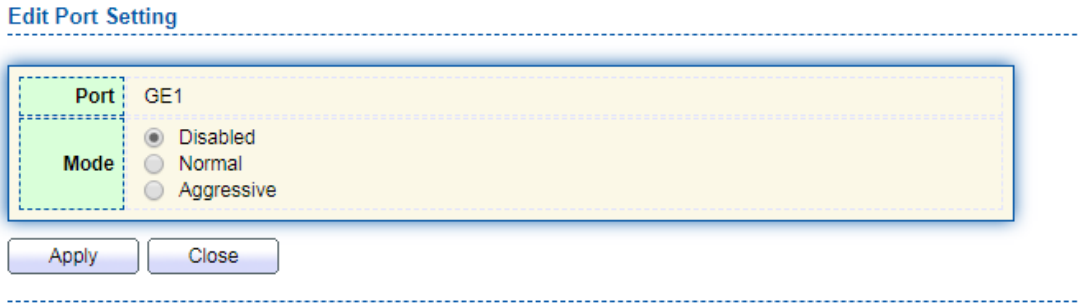
Instructions:

1. 탐색 트리에서 “Diagnostics > UDLD > Property”을 선택합니다:





2. 포트를 선택하고 “Edit” 합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
Port	Port id
Mode	UDLD port mode Disabled: 포트기능 비활성화 Normal: UDLD 는 단방향 링크를 감지하고 포트를 미확인으로 표시하여 시스템 로그를 생성 할 수 있습니다 Aggressive: UDLD 는 단방향 링크를 감지할 수 있습니다. 링크 재구축을 시도하고 8 초동안 UDLD 메시지를 계속해서 보냅니다. UDLD 에코 응답이 없는 경우 포트는 errdisable 상태가 됩니다.

17.6.2 Neighbor

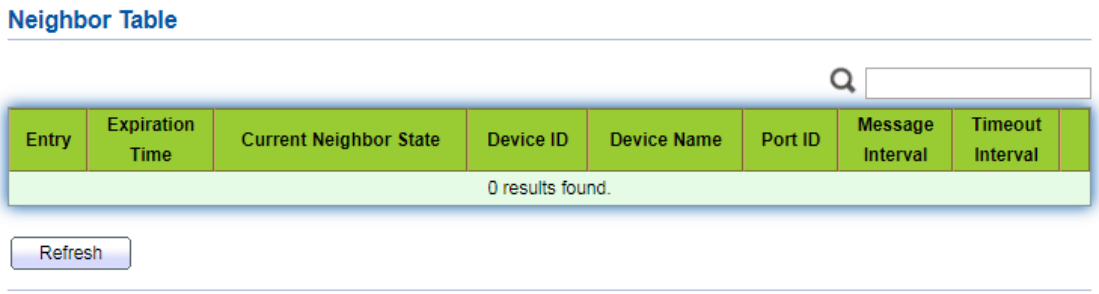
UDLD 는 각 활성 인터페이스에서 정기적으로 Hello 패킷(광고 또는 프로브라고도 함)을 보냅니다.

스위치가 Hello 패킷을 수신하면 에이징 시간이 만료될 때까지 메시지가 저장됩니다. 에이징 시간이 만료되기 전에 Hello 가 다시 수신되면 에이징 시간이 새로 고쳐집니다.

새 이웃 또는 이웃이 캐시 재동기화를 요청하면 일련의 UDLD 프로브 / 에코 (Hello) 패킷이 전송됩니다.

Instructions:

1. 탐색 트리에서 “Diagnostics > UDLD > Neighbor” 을 선택하고, 테스트할 포트를 지정합니다:



구성 항목은 다음과 같습니다.

구성 항목	설명
Entry	이웃(neighbor)의 Serial No.
Expiration Time	남은 에이징 시간
Current Neighbor State	이웃(neighbors) 현황
Device ID	이웃(neighbors)의 Device ID
Device Name	이웃(neighbors)의 Device name
Port ID	연결된 인터페이스의 ID
Message Interval	이웃(neighbors)에 대한 메시지 간격
Timeout Interval	이웃(neighbors)에 대한 시간 초과 간격

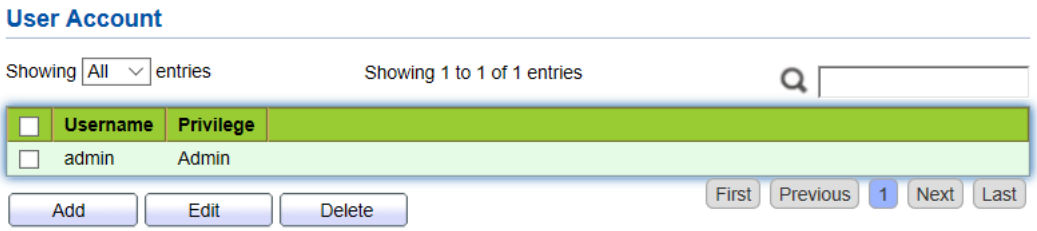
18 Management

18.1 User Account

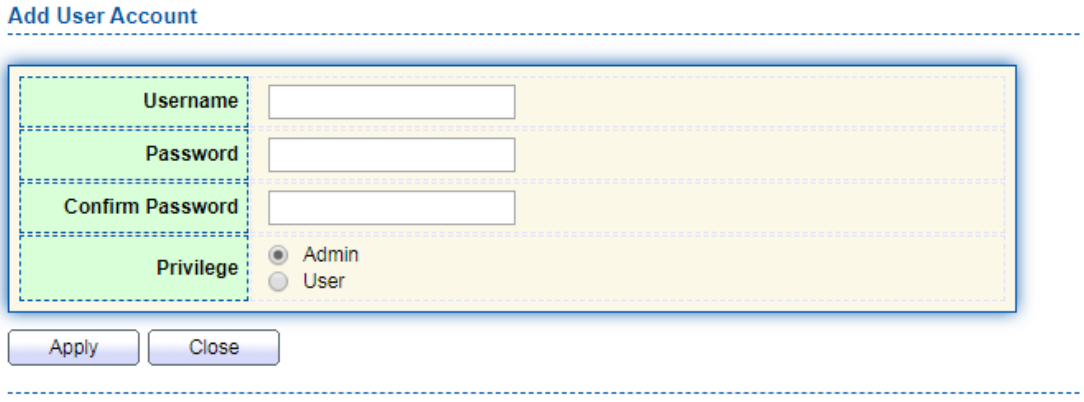
사용자는 Username 과 Password 를 수정할 수 있습니다.

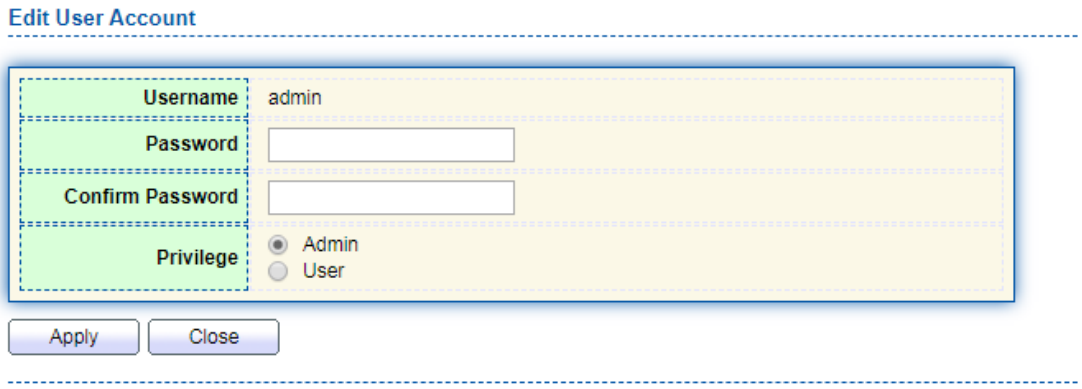
Instructions:

1. 탐색 트리에서 “Management > User Account”을 선택하고, 수정할 계정을 확인합니다:



2. 새 이용자 계정을 “Add”하고, 선택한 계정을 “Edit”합니다:

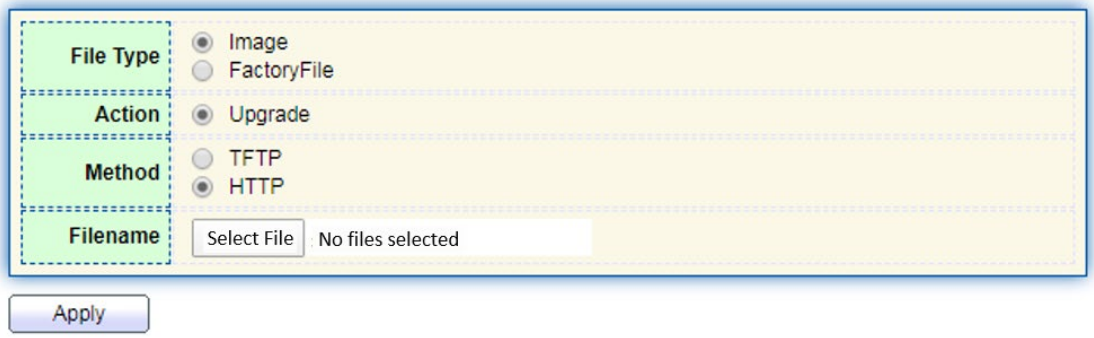




18.2 Firmware

시스템 펌웨어를 업그레이드 합니다.

Instructions:
1. 탐색 트리에서 “Management > Firmware > Upgrade” 을 선택합니다:

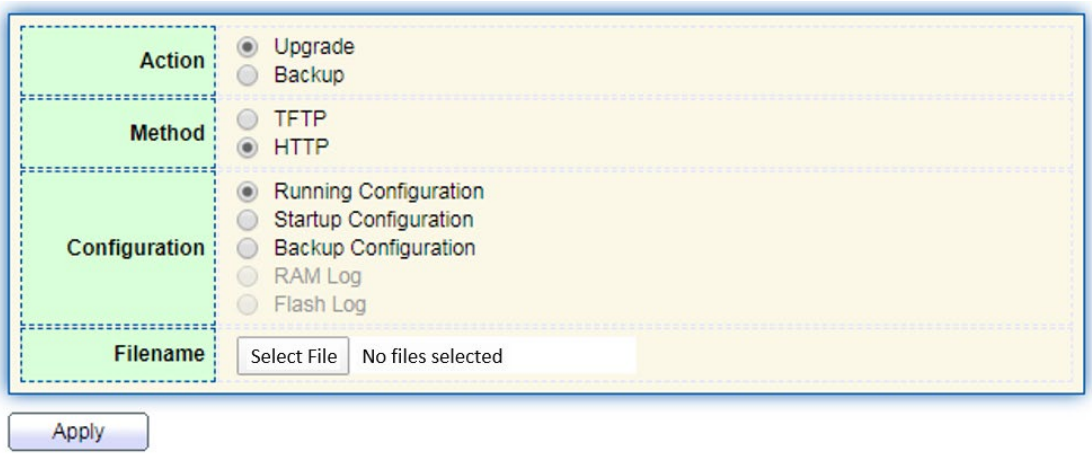


18.3 Configuration

18.3.1 Upgrade

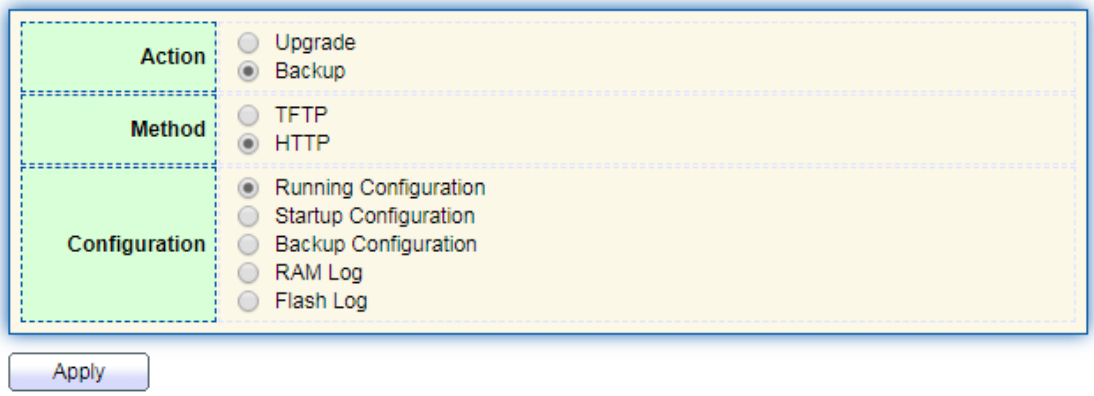
시스템 설정을 업그레이드 하거나 백업합니다.

설정 업그레이드 방법:
1. 탐색 트리에서 “Management > Configuration > Upgrade”을 선택하고, Action 을 “Upgrade”로 지정하고, “TFTP” 또는 “HTTP”을 선택합니다. 해당 파일을 선택하고, “Apply”하여 완료합니다:



설정 파일 백업 방법:

Action 을 "Backup"으로 지정하고, "TFTP" 또는 "HTTP"을 선택합니다. 해당 파일을 선택하고, "Apply"하여 완료합니다:

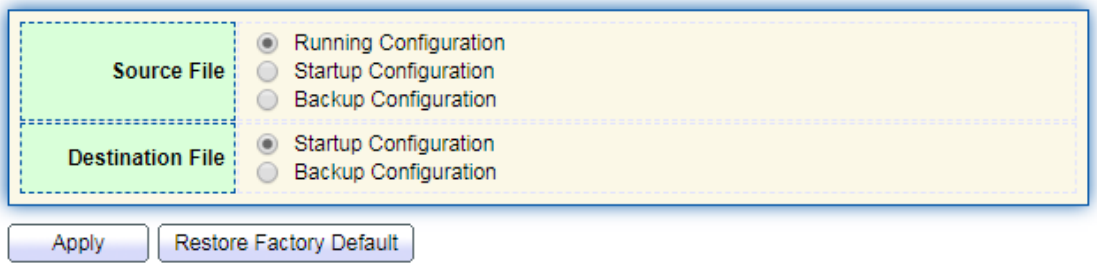


18.3.2 Save Configuration

시스템 설정을 저장하거나 공장 초기화합니다.

Instructions:

1. 탐색 트리에서 "Management > Configuration > Save Configuration"을 선택합니다:

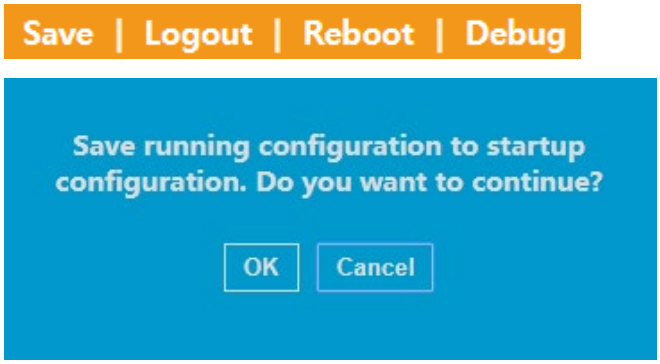


Note:

- 제품 설정 초기화를 위해서는 “Factory Reset”을 클릭하고, “Device Restart”를 해야합니다

“Running Configuration”을 “Start Configuration”이나 “Backup Configuration”으로 저장할 수 있습니다.

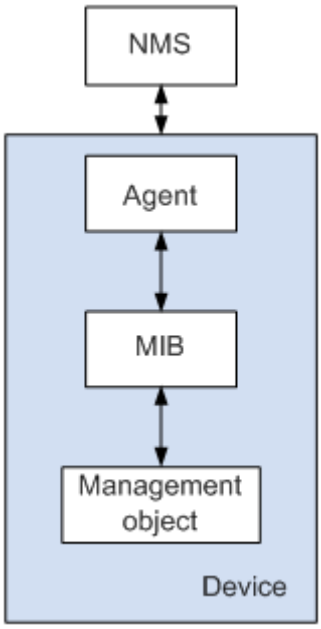
시스템 설정 저장을 위한 다른 방법:
2. 화면 우측 상단에서 “Save”을 클릭하고, “running configuration”을 “start configuration”으로 저장합니다.



18.4 SNMP

SNMP (Simple Network Management Protocol)는 **TCP / IP** 네트워크에서 널리 사용됩니다. 네트워크 관리 소프트웨어 (예 : 네트워크 관리 워크 스테이션)를 운영하는 중앙 컴퓨터로 장치를 관리합니다. **SNMP** 는 다음과 같습니다:

- Simple: 폴링 구동 **SNMP** 는 빠른 속도와 저렴한 비용으로 소규모 환경에 적용 할 수있는 기본 기능 세트를 가지고 있습니다. 또한 **UDP** 기반 **SNMP** 는 대부분의 장치와 호환됩니다. Powerful: **SNMP** 는 관리자가 정보를 쉽게 검색, 수정 및 문제를 해결할 수 있도록 두 노드 간의 관리 정보 전송을 보장하는 것을 목표로합니다. 세 가지 공통 버전, 즉 **SNMPv1, v2c** 및 **v3** 이 있습니다. 시스템에는 **NMS** (네트워크 관리 시스템), 에이전트, 관리 개체 및 **MIB** (관리 정보베이스)가 포함됩니다.
- 관리 센터 인 **NMS** 는 모든 장치를 관리합니다. 관리중인 각 장치에는 상주 에이전트, **MIB** 및 관리 개체가 포함됩니다. **NMS** 는 **MIB** 를 작동하여 **NMS** 주문을 실행하는 관리 개체에서 실행되는 에이전트와 상호 작용합니다.



< SNMP management model>

NMS

- **NMS** 는 네트워크 관리자로서 서버에서 **SNMP** 를 통해 네트워크 장치를 관리 / 감시합니다. 에이전트에게 지정된 매개 변수를 조회하거나 수정하도록 요청할 수 있습니다. **NMS** 는 에이전트가 능동적으로 보낸 트랩을 수신하여 관리 장치의 상태를 업데이트 할 수 있습니다.

Agent

- 관리 장치의 에이전트 프로세스로 장치 데이터를 유지하고 관리 데이터를보고하여 **NMS** 요청에 응답합니다. 상담원은 **MIB Table** 을 통해 관련 주문을 처리하고 요청을받은 후 결과를 **NMS** 로 다시 전송합니다. 장치는 장애 또는 다른 이벤트가 발생하면 에이전트를 통해 현재 장치 상태와 관련된 정보를 **NMS** 로 전송하기 위해 주도권을 잡습니다.

Management object

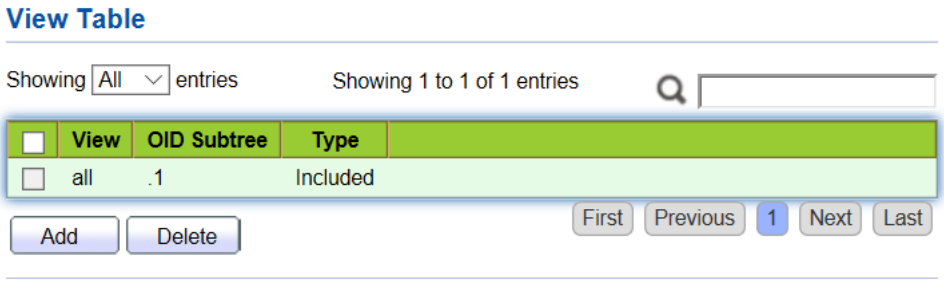
- 관리중인 개체를 의미합니다. 각 장치는 하드웨어 (예 : 인터페이스 보드), 부분 하드웨어 및 소프트웨어 (예 : 라우팅 프로토콜), 기타 구성 항목 세트를 포함하여 둘 이상의 개체를 가질 수 있습니다.

MIB

- **MIB** 는 관리 개체가 유지 관리하는 변수 (예 : 에이전트가 조회하고 설정할 수있는 정보)를 지정하는 데이터베이스입니다. **MIB** 는 이름, 상태, 액세스 권한 및 데이터 유형을 포함하여 관리 개체의 속성을 정의합니다. **MIB** 를 통해 다음 기능을 구현할 수 있습니다. 에이전트는 **MIB** 를 조회하여 인스턴트 장치 정보를 마스터하고 **MIB** 를 변경하여 상태 구성 항목을 설정합니다.

18.4.1 View

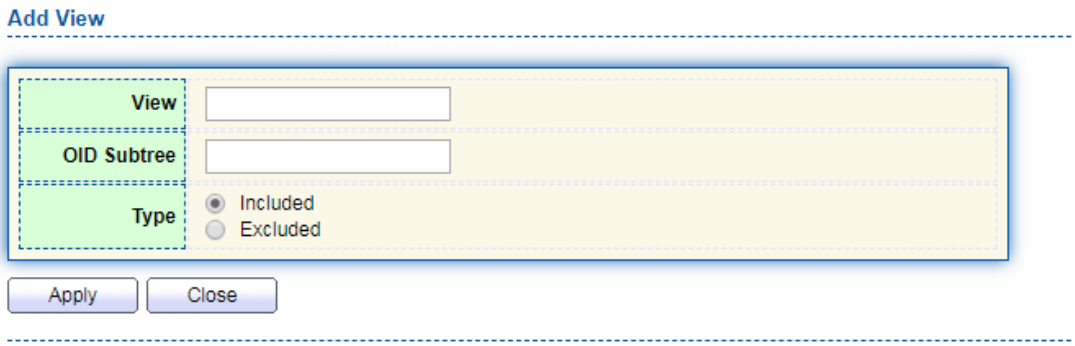
1. 탐색 트리에서 “Management > SNMP > View”을 선택합니다.



구성 항목은 다음과 같습니다.

구성 항목	설명
View	View name
OID Subtree	View OID 값
Type	View type: “Included” 또는 “Excluded”

2. 해당 설정을 “Add”하고, “Apply”하여 완료합니다.



18.4.2 Group

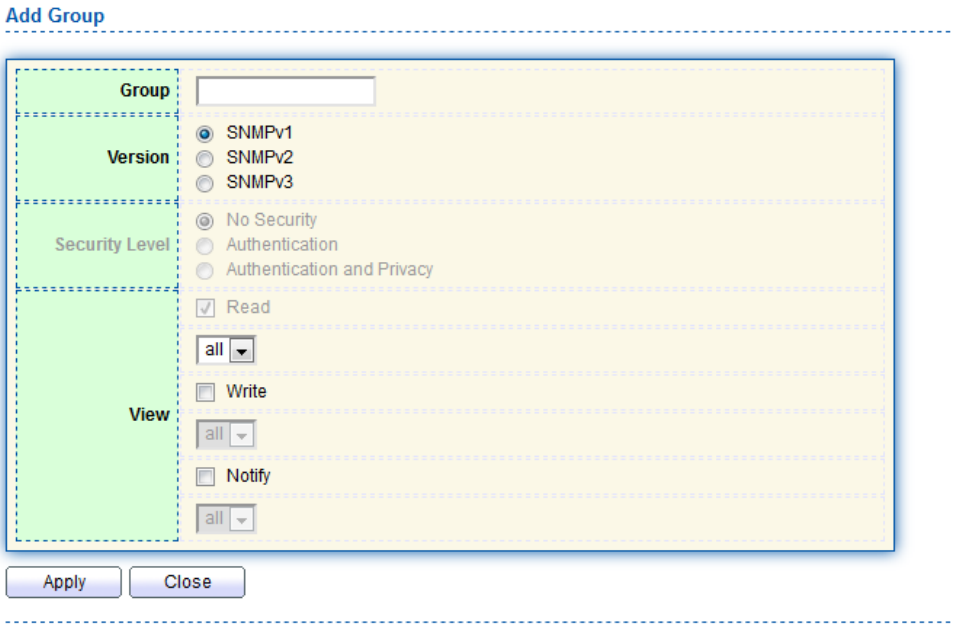
1. 탐색 트리에서 “Management > SNMP > Group”을 클릭합니다.



구성 항목은 다음과 같습니다.

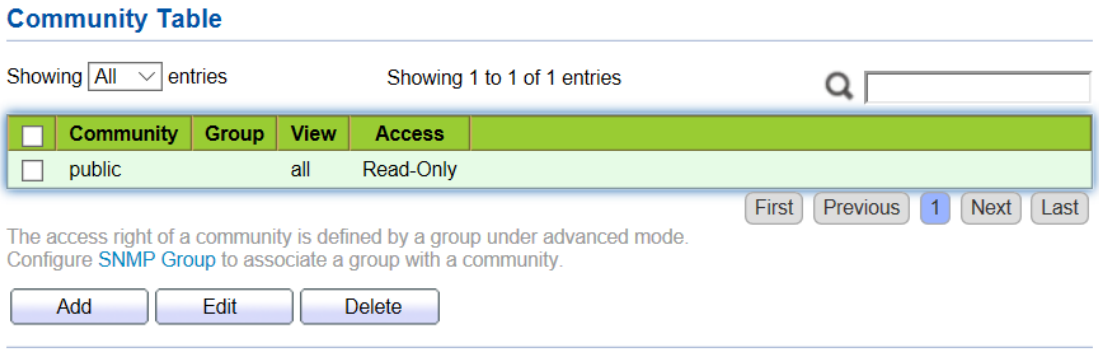
구성 항목	설명
Group	Group 이름
Version	V1, V2, V3
Security Level	Security level
View	reading, writing, notification.

2. 해당 설정을 “Add”하고, “Apply”하여 완료합니다.



18.4.3 Community

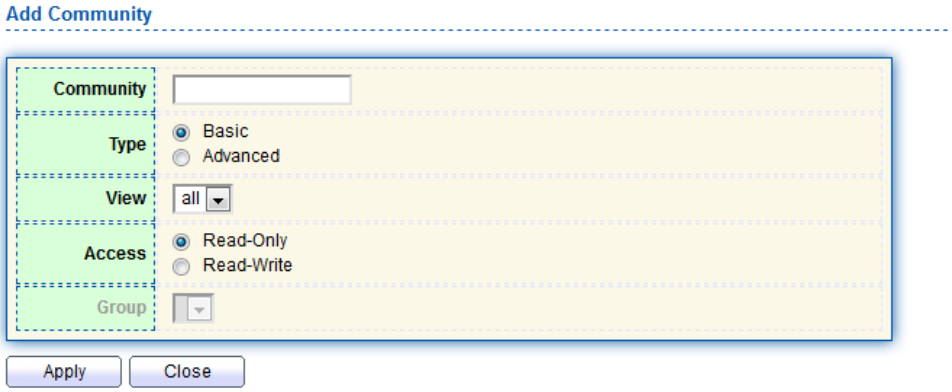
1. 탐색 트리에서 “Management > SNMP > Community”을 선택합니다.



구성 항목은 다음과 같습니다.

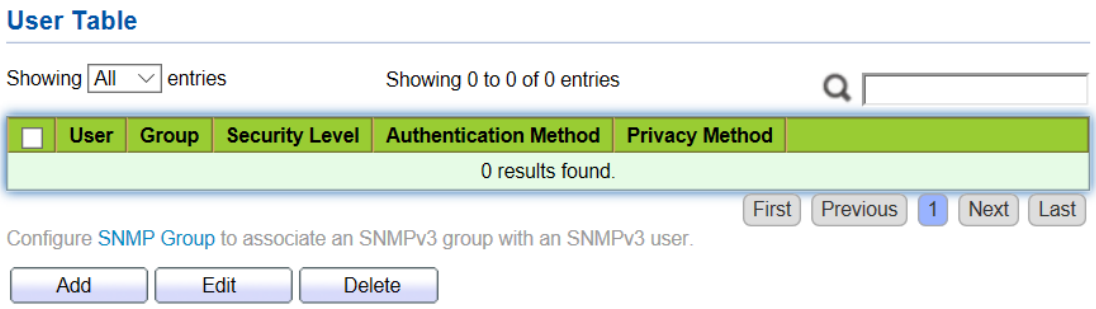
구성 항목	설명
Community	Community 설정
Group	Group 이름
View	View 이름
Access:	권한: read only 또는 read-write

2. 해당 설정을 “Add” 하고, “Apply” 하여 완료합니다.



18.4.4 User

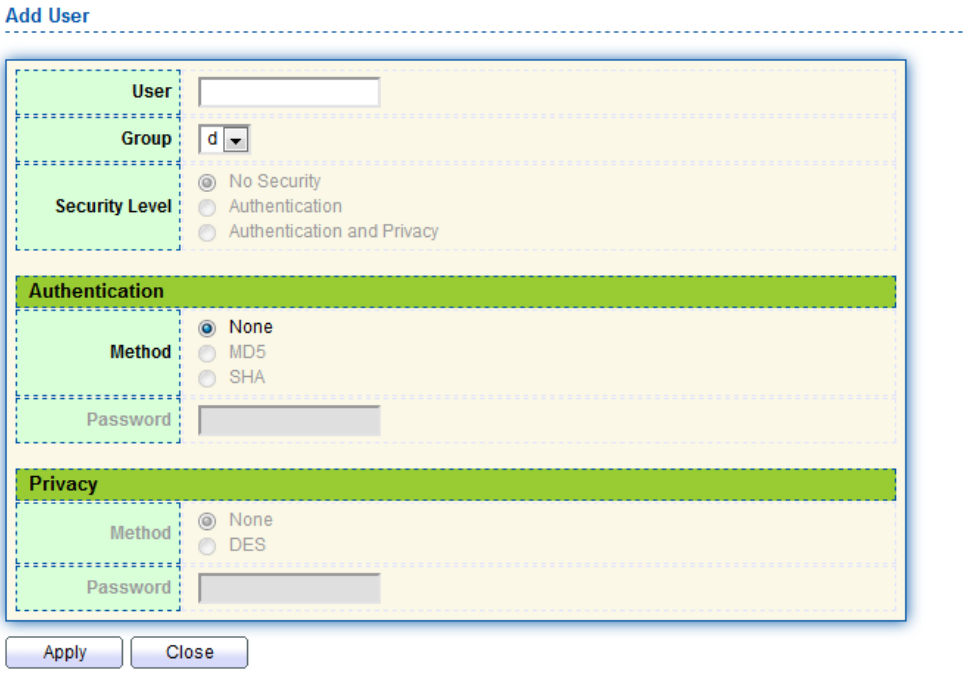
1. 탐색 트리에서 “Management > SNMP > User” 을 선택합니다.



구성 항목은 다음과 같습니다.

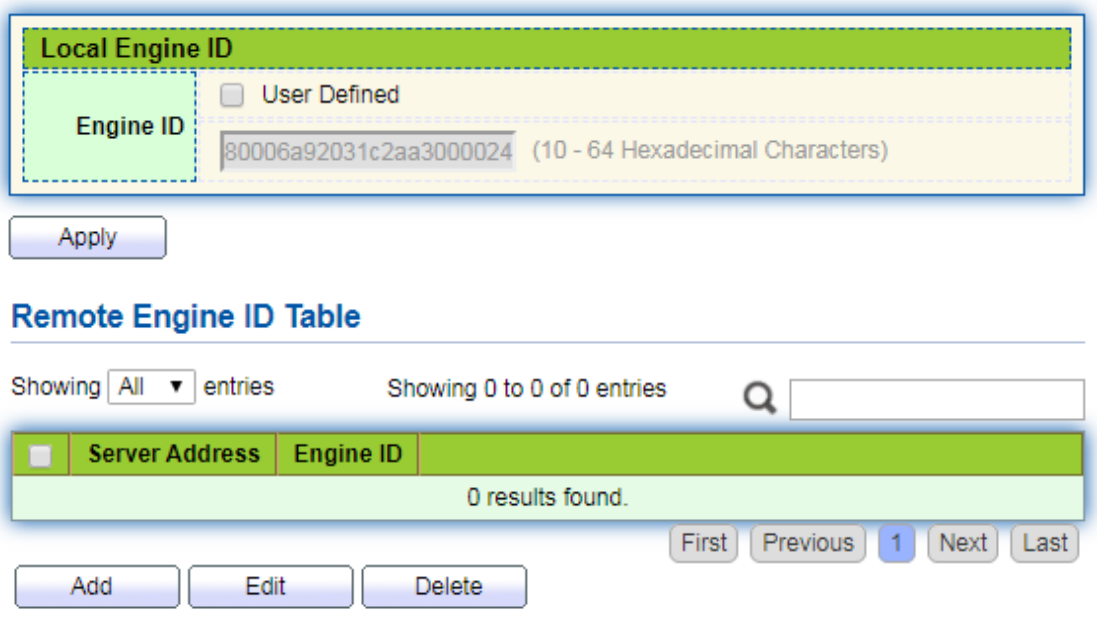
구성 항목	설명
User	Username
Group	Group name
Security Level	Security level
Authentication Method	Authentication mode
Privacy Method	Encryption mode

2. 해당 설정을 “Add” 하고, “Apply” 하여 완료합니다.



18.4.5 Engine ID

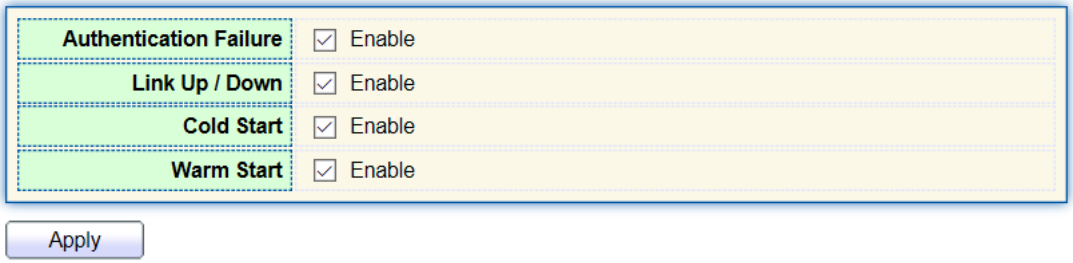
1. 탐색 트리에서 “Management > SNMP > Engine ID” 을 선택합니다.



2. “User Automation” 을 클릭하고 해당 ID 를 입력한 다음 “Apply” 하여 완료합니다.

18.4.6 Trap Event

1. 탐색 트리에서 “Management > SNMP > Trap Event”을 선택합니다.



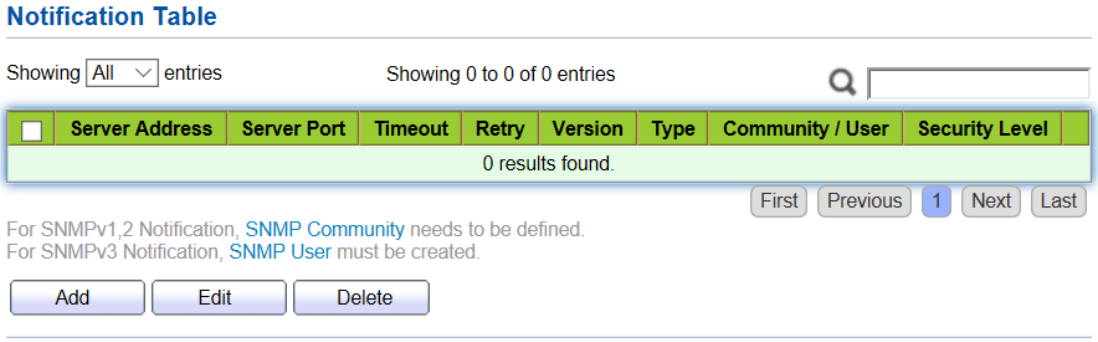
구성 항목은 다음과 같습니다.

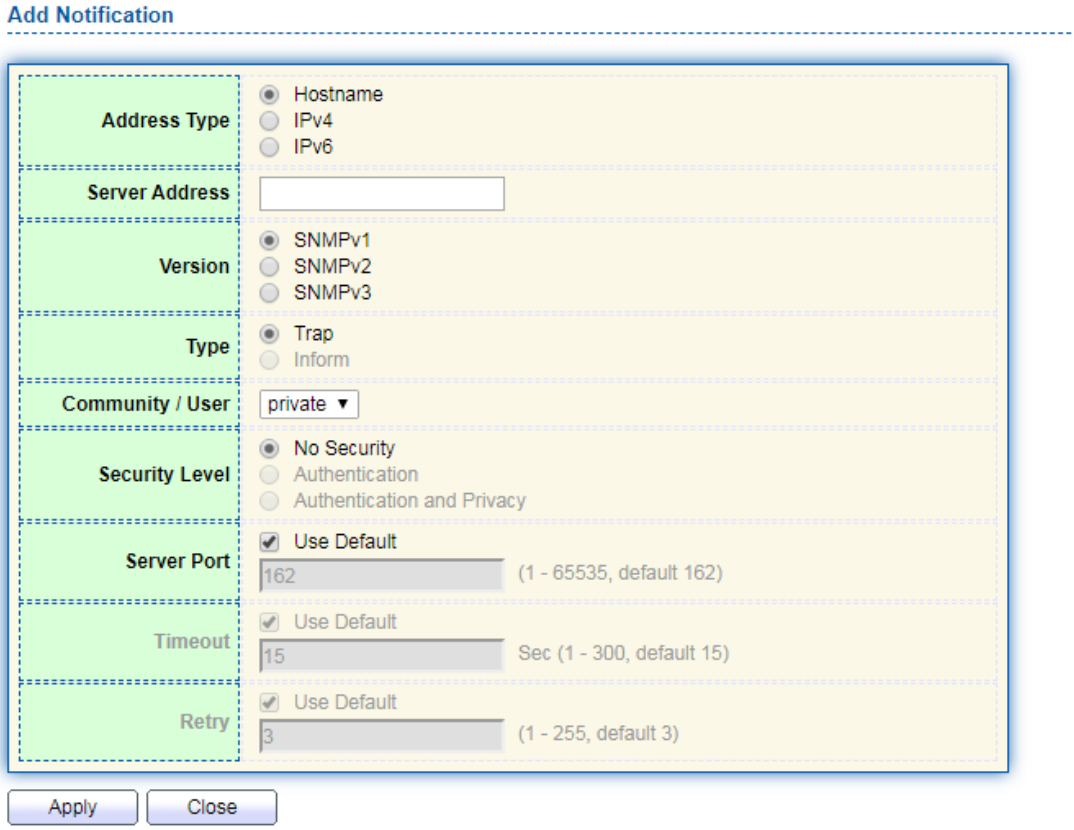
구성 항목	설정
Authentication Failure	Authentication error
Link Up / Down	Port link up/down
Cold start	Cold start
Warm start	Warm start

2. “Apply”하여 완료합니다.

18.4.7 Notification

1. 탐색 트리에서 “Management > SNMP > Notification” 을 선택합니다.





구성 항목은 다음과 같습니다.

구성 항목	설명
Address Type	Address type: “Host Name”, “IPv4” 또는 “IPv6”
Server Address	Server address 정보
Version	SNMP versions: v1, v2, v3
Type	Notification type: “Trap” 또는 “Inform”
Community / User	Community 또는 username
Security Level	Security level
Server port	1 – 65,535(기본값 162)
Timeout	1 – 300 초(기본값 15 초)
Retry	재시도 간격 1 – 255 초(기본값 3 초)

2. “Add” 하여 설정 항목을 입력합니다. “Apply”하여 완료합니다.

18.5 RMON

RMON (원격 모니터링)은 **IETF (Internet Engineering Task Force)**에서 정의한 **MIB** 이며 **MIB II** 표준을 크게 강조합니다. 주로 널리 사용되는 네트워크 관리 표준 중 하나 인 네트워크 세그먼트 또는 전체 네트워크의 데이터 흐름을 모니터링합니다.

RMON 에는 다양한 네트워크 장치에서 실행되는 **NMS** (네트워크 관리 스테이션) 및 에이전트가 포함됩니다. 네트워크 모니터 또는 탐지기에서 실행되는 **RMON** 에이전트는 포트에 연결된 네트워크 세그먼트에서 흐름 정보 (예 : 특정 기간 동안 네트워크 세그먼트의 총 메시지 수 또는 호스트로 전송 된 올바른 메시지 수)를 추적하고 계산합니다.
SNMP 아키텍처를 기반으로 **RMON** 은 기존 **SNMP** 프레임 워크와 호환됩니다. **SNMP** 는 원격 네트워크 장치를보다 효율적이고 능동적으로 모니터링하여 서브넷 작업을 감독합니다. **RMON** 은 **NMS** 와 **SNMP Agent** 간의 통신 흐름을 줄여 대규모 상호 연결 네트워크를 편리하고 효과적으로 관리 할 수 있습니다.
다중 모니터는 두 가지 방법으로 데이터를 수집 할 수 있습니다. 전용 **RMON** 프로브를 사용하여 데이터를 수집하고 **NMS** 가 정보를 직접 관리하고 네트워크 리소스를 제어합니다. 모든 **RMON MIB** 정보를 얻을 수 있습니다.
네트워크 장치 (라우터, 스위치, **HUB** 등)에 직접 액세스 할 수있는 **RMON** 에이전트는 **RMON** 프로브 기능이 있는 네트워크 시설이 됩니다. **RMON NMS** 는 **SNMP** 기본 명령을 사용하여 **SNMP** 에이전트와 데이터를 교환하여 네트워크 관리 정보를 수집합니다. 그러나 장치 자원에 의해 제한되어 일반적으로 **RMON MIB** 의 모든 데이터를 얻지 못합니다. 대부분의 장치는 알람, 이벤트, 기록 및 통계 그룹의 네 그룹에서만 데이터를 수집합니다.
영역 형 스위치는 두 번째 방식으로 **RMON** 을 실현합니다. 스위치에 직접 액세스하는 **RMON Agent** 는 **RMON** 프로브 기능이있는 네트워크 시설이됩니다.
스위치에서 지원하는 **SNMP** 에이전트를 실행함으로써 **NMS** 는 네트워크를 관리하기 위해 포트에 연결된 네트워크 세그먼트에 대한 전체 흐름, 오류 통계, 성능 통계 및 기타 정보를 얻을 수 있습니다.

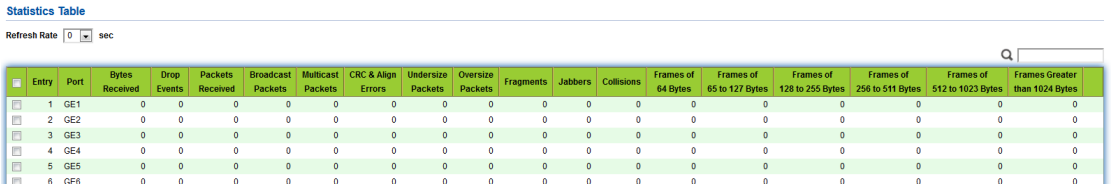
18.5.1 Statistics

통계 그룹 정보는 스위치에있는 각 모니터링 인터페이스의 통계, 즉 그룹 생성 초기부터 축적 된 정보를 반영합니다. 통계에는 네트워크 충돌 수, **CRC** 오류 메시지, 너무 작은 (너무 큰) 데이터 메시지, 브로드 캐스트 / 멀티 캐스트 메시지, 수신 된 바이트 및 메시지 등이 포함됩니다. **RMON** 통계 및 관리 기능을 통해 발생한 포트 사용 및 오류를 각각 모니터링하고 계산할 수 있습니다

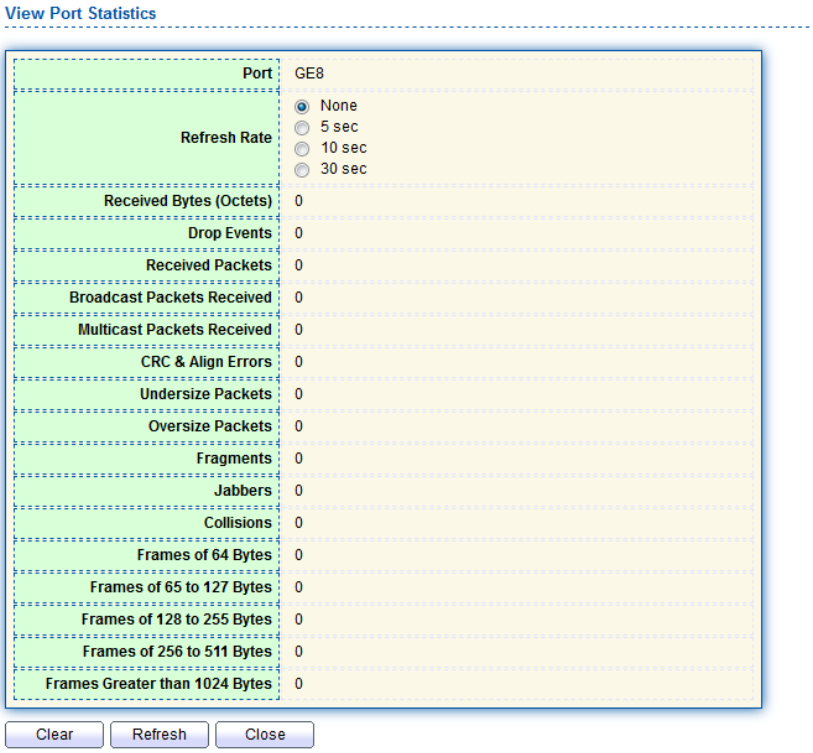
.

Instructions

1. 탐색 트리에서 “Management > RMON > Statistics”을 선택하면, 포트 관련 메시지 통계가 표시됩니다.



2. “Clear”와 “Refresh”를 하여 선택된 포트의 통계를 클리어하거나 갱신합니다. “View”를 해서 해당 정보를 확인합니다.

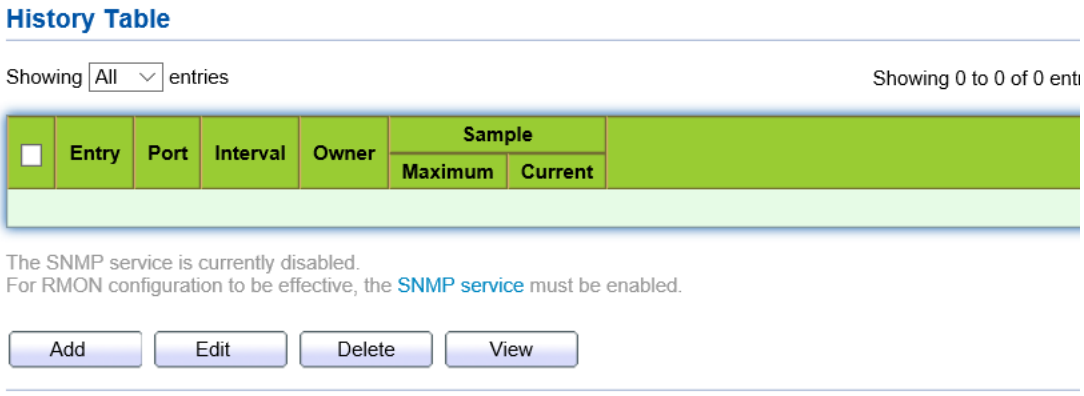


3. 갱신 주기를 설정합니다.

18.5.2 History

RMON 히스토리 그룹을 구성하면 스위치는 처리 용이성을 위해 주기적으로 네트워크 통계를 수집하고 임시로 저장하여 네트워크 세그먼트 흐름, 오류 패킷, 브로드 캐스트 패킷, 대역폭 사용률 및 기타 통계에 대한 히스토리 데이터를 제공합니다.
이력 데이터 관리는 지정된 포트의 데이터에 대한 주기적 수집 및 유지 관리를 포함하여 이력 데이터 수집 측면에서 장치를 설정하는 데 사용할 수 있습니다.

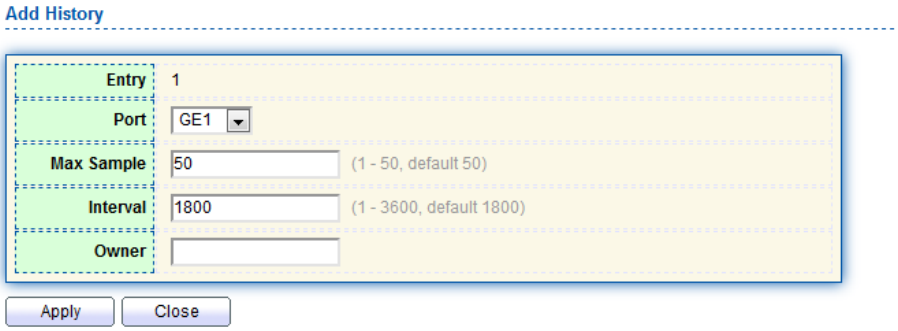
1. 탐색 트리에서 “Management > RMON > History”을 선택합니다.



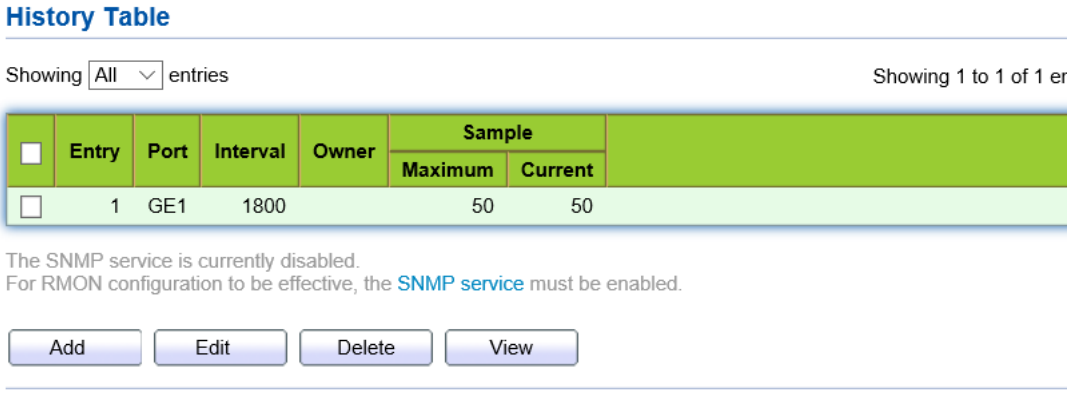
구성 항목은 다음과 같습니다.

구성 항목	설명
Entry	이벤트 그룹의 일련 번호
Port	계산할 포트
Interval	샘플링 간격은 **1 ~ 3,600** (단위 : **s**)이며 기본적으로 **1,800s** 입니다.
Owner	소유자
Maximum	최대 샘플 수는 **0** 에서 **50** 까지이며 기본값은 **50** 입니다.
Current	현재 샘플 수

2. 히스토리 그룹을 구성하기 위해 해당 구성 항목을 “Add” 합니다.



3. “Apply” 하고 다음과 같이 마칩니다.



18.5.3 Event

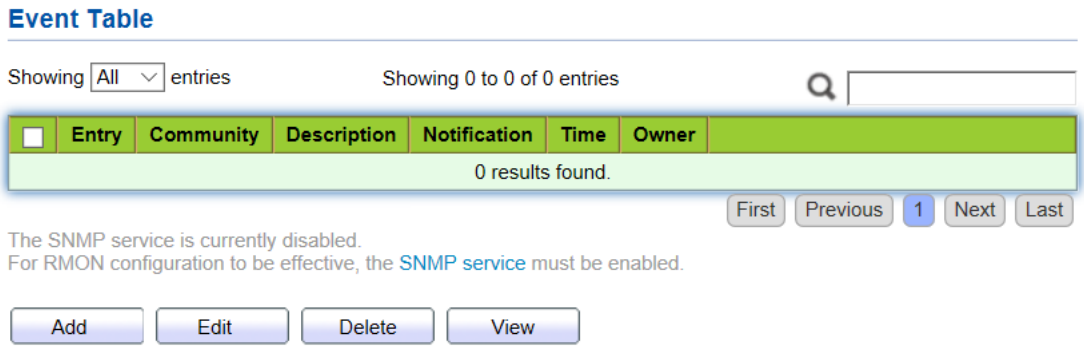
이벤트 번호 및 처리 방법을 정의하는 이벤트 그룹은 주로 알람 그룹 구성 항목 및 확장 알람 그룹 구성 항목에 의해 트리거 된 이벤트에 대한 것입니다.

이에 대한 몇 가지 해결책이 있습니다.

- 로그 테이블에 기록;
- NMS 에 트랩 메시지를 전송하는 단계;
- 로그를 기록하고 트랩 메시지를 전송하는 단계;
- 무시함

Instructions

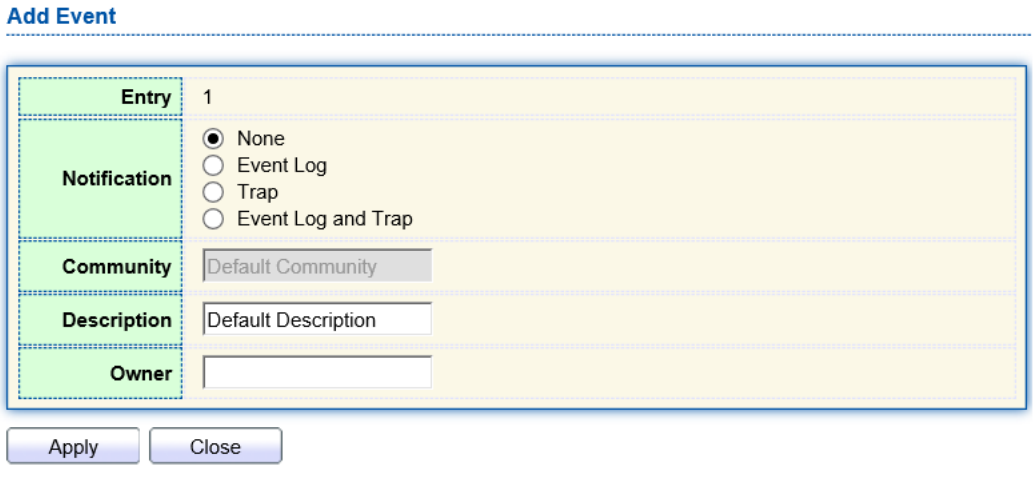
1. 탐색 트리에서 “Management > RMON > Event”을 선택합니다.



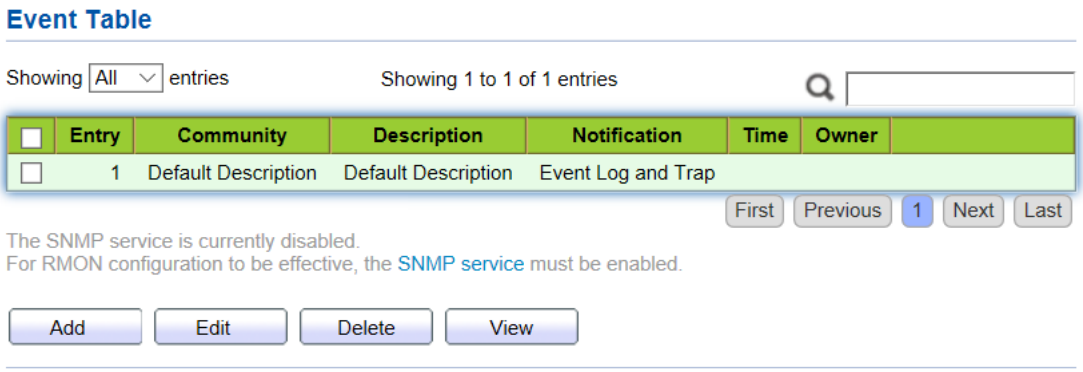
구성 항목은 다음과 같습니다.

구성 항목	설명
Entry	이벤트 그룹의 일련 번호
Community	Community name
Description	Description
Notification	Notification
Timer	Time
Owner	Owner

2. 이벤트 그룹을 구성하기 위해 해당 구성 항목을 “Add” 합니다.



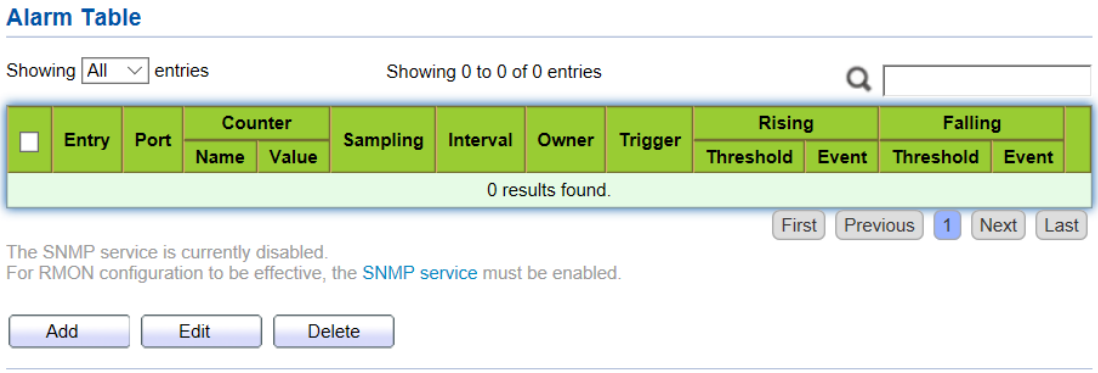
3. “Add” 하고 다음과 같이 마칩니다.



18.5.4 Alarm

RMON 경보 관리는 포트 통계와 같은 특정 경보 변수를 모니터링합니다. 모니터링 된 데이터의 값이 해당 방향에서 정의 된 임계 값을 초과하면 알람 이벤트가 발생하며, 이는 규정 된 치료 모드에 따라 처리됩니다. 이벤트 정의는 이벤트 그룹에서 실현됩니다. 사용자가 경보 항목을 정의한 후 시스템은 다음과 같이 처리합니다. 샘플링 시간에 의해 정의 된 경보 변수를 샘플링하고 값을 임계 값과 비교해야합니다. 더 높은 임계 값의 경우 해당 이벤트가 트리거됩니다.

1. 탐색 트리에서 “Management > RMON > Alarm”을 선택합니다.

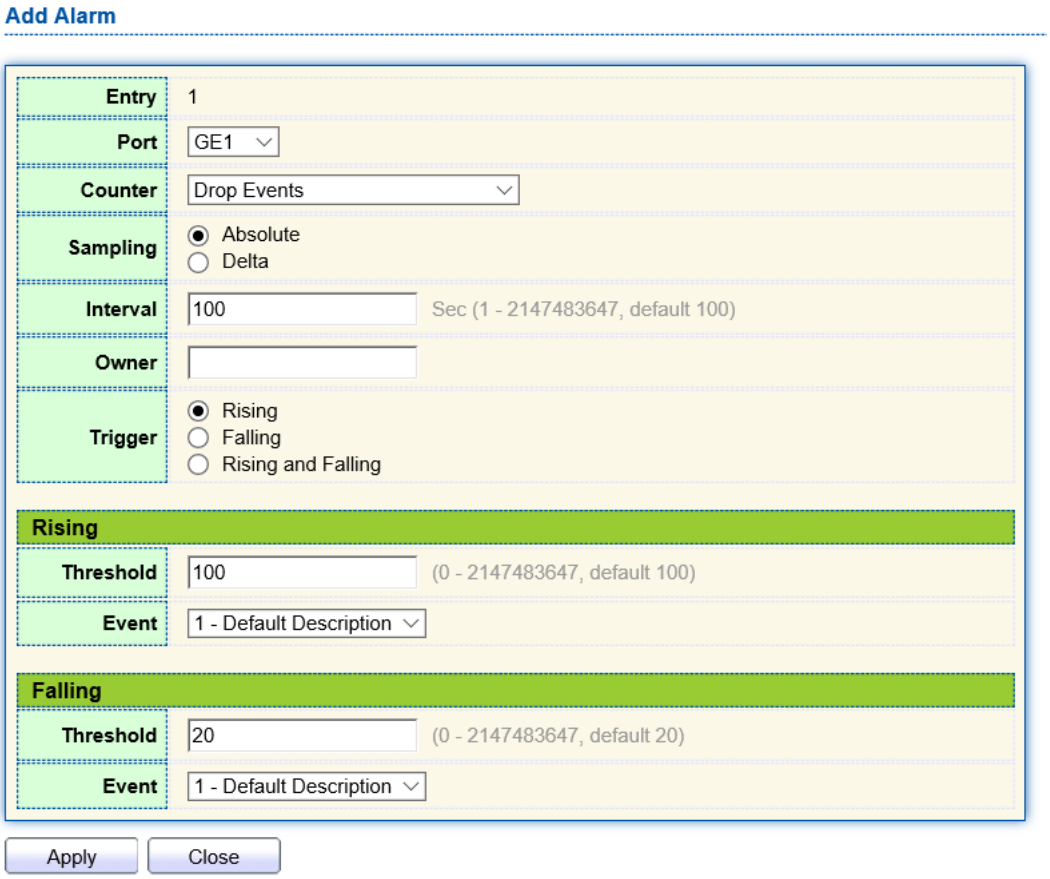


구성 항목은 다음과 같습니다.

구성 항목	설명
Entry	경보 그룹의 일련 번호
Port	계산할 포트를 입력하십시오
Counter	경보의 샘플 매개 변수
Interval	샘플링 간격 범위는 **1** 에서 **2,147,483,647** 이며 초 단위입니다. 기본적으로 **100** 초입니다.
Sampling	샘플 유형 : 절대 및 삭제
Owner	Owner

Threshold (Rising)	상승 에지의 임계 값 범위는 **0** 에서 **2,147,483,647** 입니다.
Event (Rising)	이벤트 그룹 색인. 알람이 발생하면 해당 이벤트가 활성화됩니다.
Threshold (Falling)	하강 에지의 임계 값 범위는 **0** 에서 **21,474,836,475** 입니다
Event (Falling)	이벤트 그룹 색인. 알람이 발생하면 해당 이벤트가 활성화됩니다.

2. 알람 그룹을 구성하기 위해 해당 구성 항목을 “Add” 합니다.



3. “Apply” 하고 다음과 같이 마칩니다.

