U-F9028HPH

24-Gigabit PoE Port + 4-10Gigabit SFP Port

사용자 매뉴얼

Ver. 1.0

Revision history

Date	Version	Description
Apr 13 2023	V 1.0	The first edition

Contents

1 머리말

1.1 대상 고객

이 매뉴얼은 네트워크 설치, 구성 및 유지 관리를 담당하는 설치자 및 시스템 관리자를 위해 작성되었습니다. 이는 사용자가 모든 네트워크 통신 및 관리 프로토콜뿐만 아니라 네트워킹과 관련된 기술 용어, 이론적 원리, 실무 기술 및 장치, 프로토콜 및 인터페이스의 전문 지식을 이해했다고 가정합니다. 그래픽 사용자 인터페이스(GUI), 명령줄 인터페이스, 단순 네트워크 관리 프로토콜(SNMP) 및 웹 탐색기에 대한 업무 경험도 필요합니다.

2 웹페이지 로그인

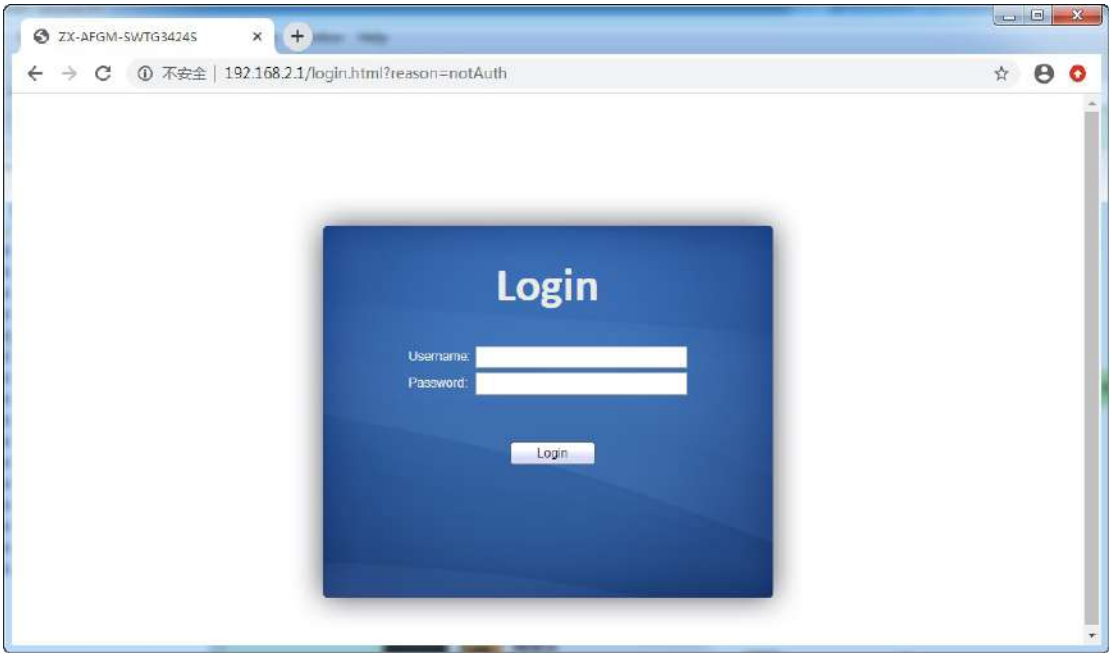
2.1 네트워크 관리 클라이언트에 로그인

기본 스위치 주소(http://192.168.2.1)를 입력하고 "Enter"를 누릅니다.

🕮 브라우저 표준: IE 9.0, Chrome 23.0 및 Firefox 20.0 이상.

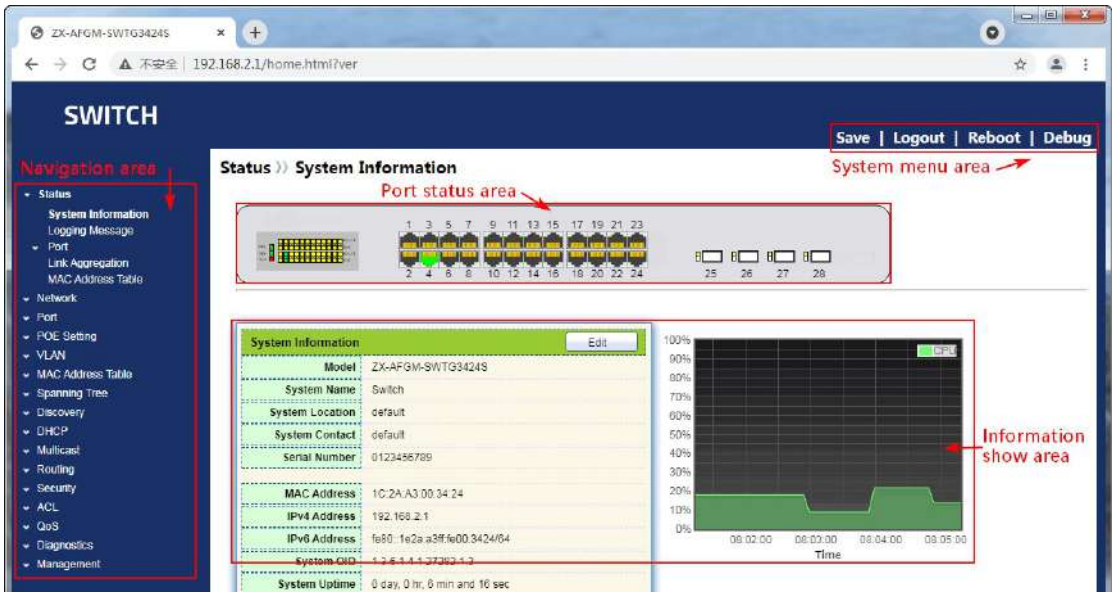
PC 의 IP 네트워크 세그먼트를 스위치의 IP 네트워크 세그먼트와 일치하게 유지하되 로그인할 때 IP 주소를 구별하십시오. 첫 번째 로그인의 경우 PC 의 IP 주소를 192.168.2.x 로 설정하고 서브넷 마스크를 255.255.255.0 으로 설정하십시오(1< x ≤254).

아래와 같이 로그인 창이 나타납니다. 기본 사용자 이름 "admin"과 비밀번호 "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 모음

상태, 네트워크, 포트, PoE 설정, VLAN, MAC 주소 테이블, 스패닝 트리, 검색, DHCP, 멀티캐스트, 라우팅, 보안, ACL, QoS, 진단 및 관리와 같은 메뉴 항목을 웹 네트워크 관리 클라이언트에서 사용할 수 있습니다. 각 항목에는 하위 메뉴가 포함되어 있습니다. 탐색 표시줄은 다음과 같이 자세히 설명됩니다.

메뉴 아이템	서브 메뉴	하위 서브 메뉴	설명
Status	System Information		포트 상태 및 제품 정보 표시
	Logging Message		장치 실행 및 작업 로그 표시
	Port	Statistics	자세한 포트 통계 표시
		Error Disabled	포트에 발생한 장애를 표시합니다.
		Bandwidth Utilization	모든 포트의 단위 시간당 대역폭 사용량을 표시합니다.
	Link Aggregation		집계 그룹 상태 및 구성원 표시
	MAC Address Table		현재 장치의 MAC 주소 테이블을 표시합니다.
Network	IP Address		관리 IP 주소 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		포트 오류 비활성화 보호 구성 및 보기
	Link Aggregation	Group	LAG 에 포함된 포트 및 전략 밸런싱 알고리즘 구성 및 보기
		Port Setting	LAG 구성 및 보기
		LACP	LACP 시스템 우선순위 및 포트 구성 확인
	EEE		EEE 상태 및 정보 구성 및 보기
	Jumbo Frame		시스템이 전달하는 최대 메시지 길이를 구성하고 확인합니다.
	Port Security		포트 보안의 속도 제한과 포트 상태를 구성하고 확인합니다.
	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 포트의 타이밍 스위치 구성 및 보기
	PoE Port Timer Reboot Setting		Poe 포트 예약된 재시작 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	프로퍼티	Voice-VLAN 기능 및 포트 상태 정보 구성 및 보기
		Voice OUI	Voice-VLAN OUI 정보 구성 및 보기
	Protocol VLAN	Protocol Group	프로토콜 VLAN 그룹 구성 및 보기
		Group Binding	프로토콜 VLAN 포트 및 그룹 바인딩을 구성하고 확인합니다.

	MAC VLA	MAC Group	MAC VLAN 그룹 구성 및 보기
		Group Binding	MAC VLAN 포트 및 그룹 바인딩 구성 및 보기
	Surveillance VLAN	프로퍼티	감시-VLAN 기능 및 포트 상태 정보 구성 및 보기
		Surveillance OUI	감시-VLAN OUI 정보 구성 및 보기
	GVRP	프로퍼티	기능적 전역 및 포트 상태 구성 및 보기
		Membership	학습된 VLAN 과 포트 멤버 구성 및 보기
		Statistics	포트와 관련된 메시지 통계 구성 및 보기
MAC Address Table	Dynamic Address		장치의 동적 MAC 주소와 에이징 시간을 구성하고 확인합니다.
	Static Address		장치의 정적 MAC 주소 테이블 구성 및 보기
	Filtering Address		필터링할 MAC 주소 테이블 구성 및 보기
	Port Security Address		포트 보안으로 학습된 MAC 주소 테이블 구성 및 보기
Spanning Tree	프로퍼티		STP 상태 및 속성 구성 및 보기
	Port Setting		STP 의 포트 특성 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	프로퍼티	LLDP 관련 속성 구성 및 보기
		Port Setting	각 포트에서 LLDP 의 전송 및 수신 상태를 구성하고 확인합니다.
		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 메시지의 송수신 상태를 구성하고 확인합니다.
DHCP	프로퍼티		DHCP 서비스 스위치 및 포트 스위치 구성 및 보기
	IP Pool Setting		DHCP 서버 IP 주소 풀 구성 및 보기
	VLAN IF Address Group Setting		VLANIF 및 DHCP 서버 그룹 바인딩 관계 구성 및 보기
	Client List		DHCP 클라이언트 목록 보기
	Client Static Binding Table		DHCP 클라이언트 정적 바인딩 테이블 항목 구성 및 보기
Multicast	General	프로퍼티	기능 구성 구성 및 보기
		Group Address	관련 정적 멀티캐스트 정보 구성 및 보기
		Router Port	멀티캐스트 라우팅 포트 정보 구성 및 보기
		Forwarding All	멀티캐스트 전달 포트 정보 구성 및 보기
		Throttling	각 포트에서 멀티캐스트 제한 구성 및 보기
		Filtering Profile	필터링된 멀티캐스트 주소 구성 및 보기
		Filtering Binding	필터링 규칙 및 포트와 관련된 바인딩 정보 구성 및 보기
	IGMP Snooping	프로퍼티	스위치, 버전 등을 구성하고 확인합니다.
		Querier	쿼리자 상태 구성 및 보기
		Statistics	프로토콜 메시지 구성 및 보기
	MLD Snooping	프로퍼티	프로토콜, 스위치 등을 구성하고 확인합니다.
		Statistics	프로토콜 메시지 구성 및 보기
	MVR	프로퍼티	스위치 등의 속성 정보 구성 및 보기
		Port Setting	각 포트의 상태 구성 및 보기
		Group Address	기능, VLAN 및 그룹 주소 구성

			및 보기
Routing	IPv4 Management and Interfaces	IPv4 Interface	VLANIF IPv4 주소 정보 구성 및 보기
		IPv4 Routes	IPv4 고정 경로 구성 및 보기
		ARP	ARP 테이블 구성 및 보기
	IPv6 Management and Interfaces	IPv6 Interface	VLANIF IPv6 인터페이스 정보 구성 및 보기
		IPv6 Address	VLANIF IPv6 주소 정보 구성 및 보기
		IPv6 Routes	IPv6 고정 경로 구성 및 보기
		IPv6 Neighbors	IPv6 인접 테이블 구성 및 보기
	Rip Routes Management	Rip Routes Setting	RIP 경로 구성 및 보기
	Ospf Routes Management	Ospf Routes Setting	OSPF 경로 구성 및 보기
Security	RADIUS		RADIUS 서버 관련 정보를 볼 수 있도록 구성
	TACACS+		TACACS+ 서버 관련 정보를 볼 수 있도록 구성
	AAA	Method List	로그인 인증 방법 구성 및 보기
		Login Authentication	단말기의 인증 방법 구성 및 보기
	Management Access	Management VLAN	관리 VLAN 구성 및 보기
		Management Service	서비스 관리 모드 및 관련 속성 구성 및 보기
		Management ACL	관리 채널을 목표로 하는 ACL 구성 및 보기
		Management ACE	관리 채널의 ACE 구성 구성 및 보기
	Authentication Management	프로퍼티	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	프로퍼티	스위치 옵션 구성 및 보기

		Port Setting	포트에서 스위치 옵션 구성 및 보기
	Dynamic ARP Inspection	프로퍼티	동적 ARP 검사 구성 및 보기
		Statistics	각 포트에서 APR 검사 상태의 메시지 통계를 구성하고 확인합니다.
	DHCP Snooping	프로퍼티	스위치와 상태 구성 및 보기
		Statistics	각 포트에서 수신한 DHCP 메시지 통계를 구성하고 확인합니다.
		Option82 프로퍼티	옵션 82 와 관련된 속성 구성 및 보기
		Option82 Circuit ID	옵션 82 의 회로 ID 구성 및 보기
	IP Source Guard	Port Setting	포트의 상태 구성 및 보기
		IMPV Binding	IP, MAC, 포트 및 VLAN 의 바인딩 테이블 구성 및 보기
		Save Database	바인딩 테이블 항목의 저장소와 정보를 구성하고 확인합니다.
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	프로퍼티	QoS 스위치 및 상태 구성 및 보기
		Queue Scheduling	대기열 예약 알고리즘 구성 및 보기
		CoS Mapping	우선순위 및 로컬 대기열 매핑 테이블 구성 및 보기
		DSCP Mapping	우선순위 및 로컬 대기열 매핑 테이블 구성 및 보기
		IP Precedence Mapping	우선순위 및 로컬 대기열 매핑 테이블 구성 및 보기

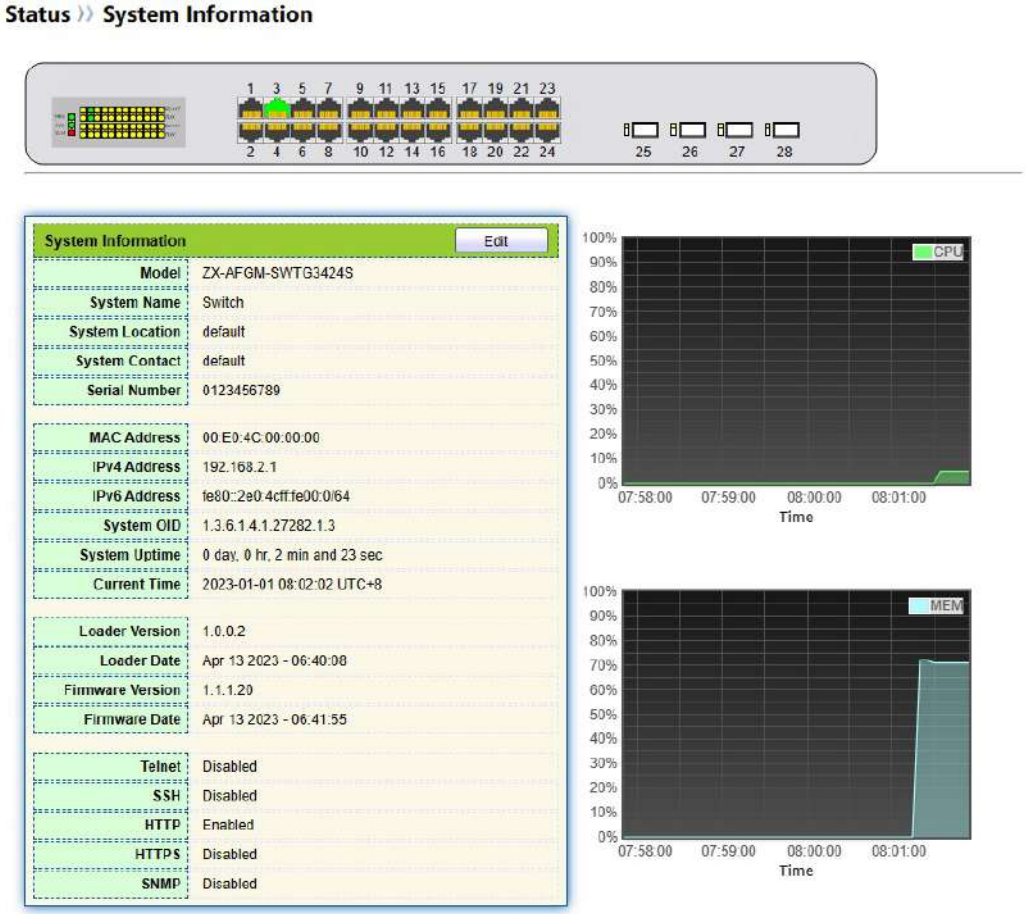
	Rate Limit	Ingress/Egress Port	포트 속도 제한 구성 및 보기
		Egress Queue	송신 대기열을 기반으로 속도 제한 구성을 구성하고 확인합니다.
Diagnostics	Logging	프로퍼티	스위치와 상태 구성 및 보기
		Remote Server	원격 서버의 주소 구성 및 보기
	Ping		Ping 을 통한 네트워크 진단
	Traceroute		Traceroute 를 통한 네트워크 진단
	Copper Test		VCT 를 통한 전기 인터페이스 링크 진단
	Fiber Module		광 인터페이스에서 SFP 모듈을 확인하십시오.
	UDLD	프로퍼티	스위치와 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	실행 중인 장치를 지원하는 구성 파일을 저장합니다.
	SNMP	View	SNMP 기능 보기 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 상태

3.1 시스템 정보

연결된 스위치에 따라 웹 네트워크 관리 패널에는 포트 수, 포트 상태, 제품 정보, 장치 상태, 기능 켜짐-꺼짐 상태 등을 포함한 포트 및 제품 정보가 직접 표시됩니다.

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

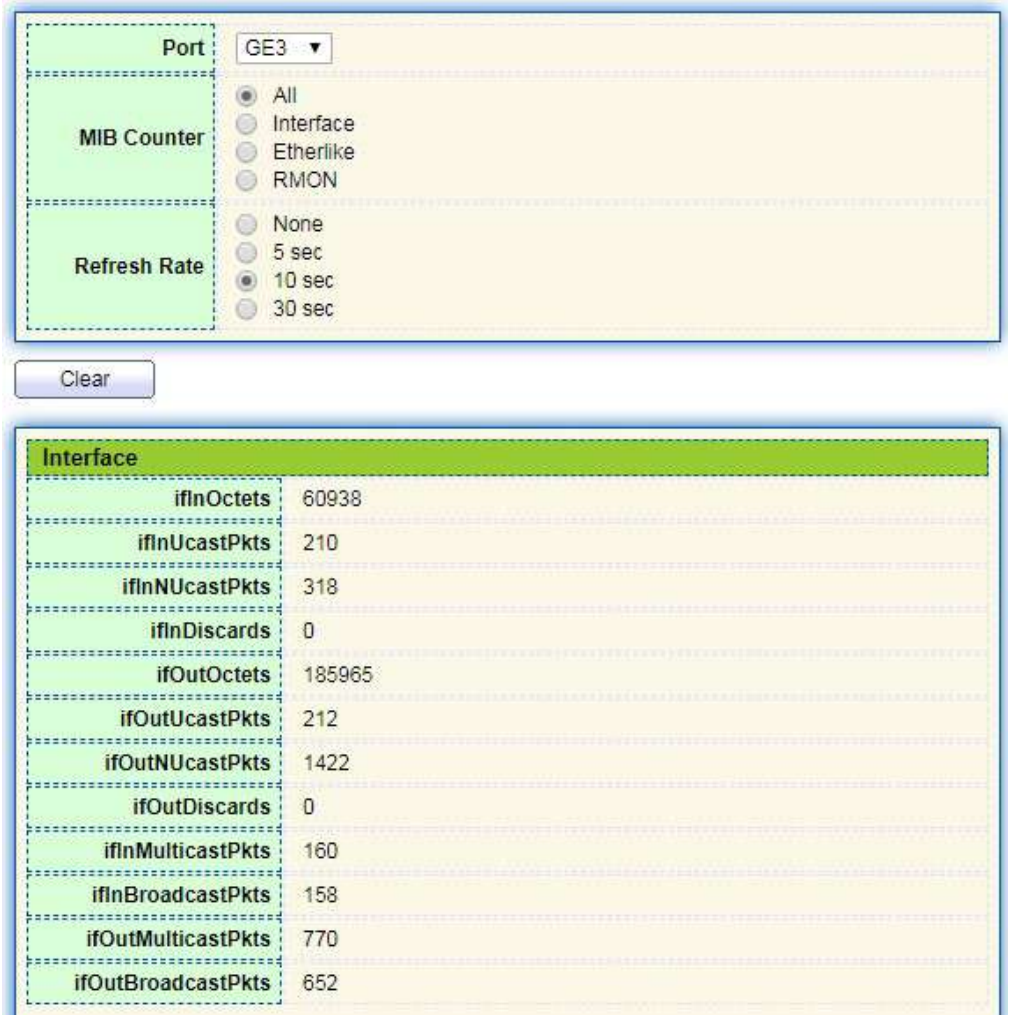


포트에 마우스를 올리면 포트번호, 종류, 속도, 상태를 확인할 수 있습니다. 제품 정보에서 "시스템 이름", "위치" 및 "연락처"를 "편집"합니다. "적용"하고 마무리합니다.

3.2 통계

포트의 자세한 흐름 통계와 사용자가 수동으로 새로 고치거나 지울 정보를 소개합니다.

1. 다음과 같이 탐색 표시줄에서 " Status > Port > Statistics "를 클릭합니다.



현재 포트의 흐름 통계를 "지우고" 페이지를 새로 고칩니다.

3.3 맥 주소 테이블

MAC 주소 테이블 정보 보기

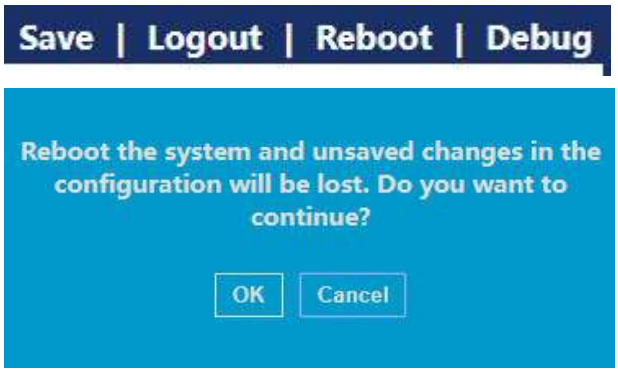
1. 다음과 같이 탐색 표시줄에서 “Status > MAC Address Table”을 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

Query Items	설명
MAC	대상 MAC 주소
VLAN	MAC 주소에 속하는 VLAN ID
Port	MAC 주소에 해당하는 메시지 송신
Type	동적 MAC 주소는 설정된 에이징 시간에 따라 에이징되는 항목을 나타냅니다. 스위치는 MAC 주소 학습 메커니즘이나 수동 생성을 기반으로 항목을 추가할 수 있습니다. 정적 MAC 주소는 수동으로 구성되고 노화되지 않는 지정된 테이블을 나타냅니다. 관리 MAC 주소는 관리 포트의 주소를 나타냅니다.

3.4 재시작

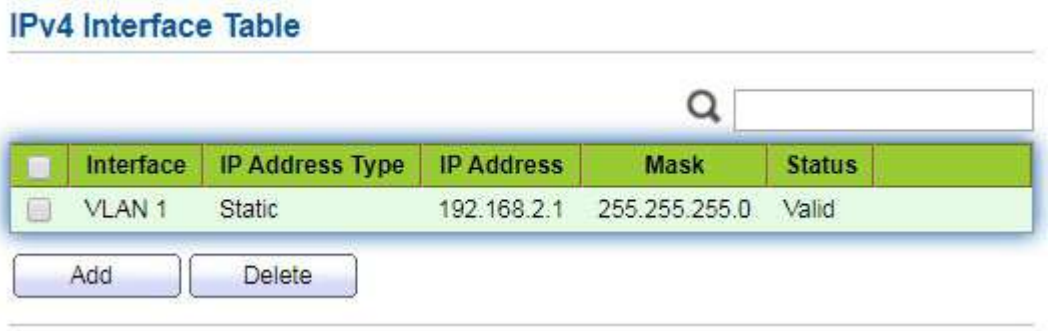
1. 다음 안내에 따라 오른쪽 상단의 '재부팅'을 클릭하세요.



3.5 관리 IP 주소

웹 인터페이스에서 관리 IP 주소를 변경합니다.

1. Click the “Routing > IPv4 Management and Interfaces > IPv4 Interface” 탐색 모음에서 다음과 같이 기본적으로 IPv4 주소 192.168.2.1/24 를 검색합니다.

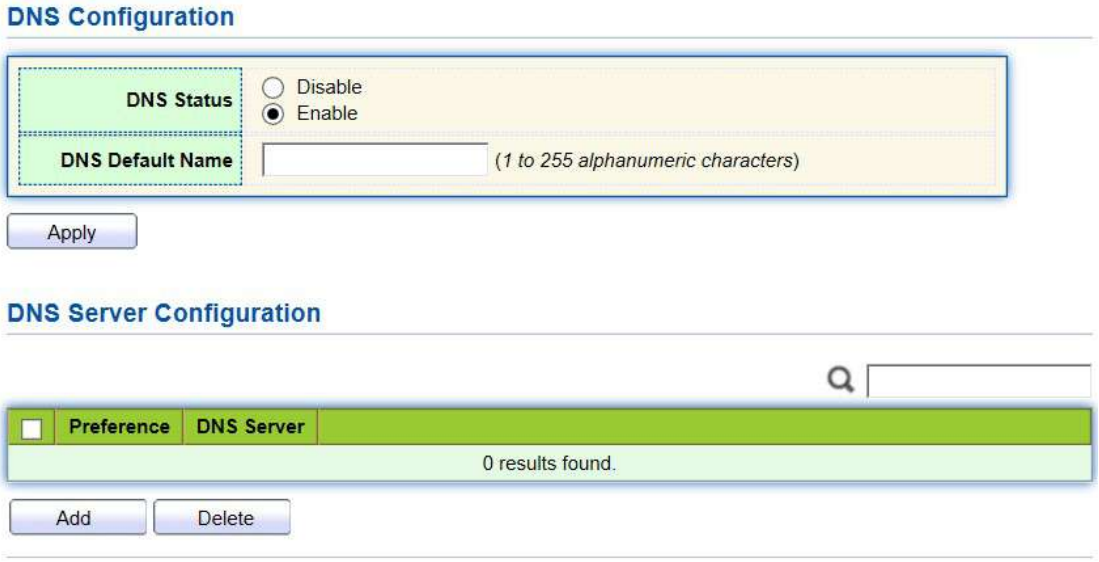


4 네트워크

4.1 DNS

DNS 는 도메인 이름 시스템(Domain Name System)의 약어로, 단위에서 도메인 계층까지 컴퓨터와 네트워크 서비스의 이름을 지정합니다. 도메인 이름은 각각 고유한 IP 주소에 해당하는 일련의 단어나 약어로 구분된 점으로 구성됩니다. DNS 는 도메인 이름을 확인하는 인터넷상의 서버입니다. 인터넷 및 기타 TCP/IP 네트워크에 적용 가능한 DNS 이름은 사용자에게 친숙한 이름을 통해 컴퓨터와 서비스를 검색합니다. 핵심 인터넷 서비스 중 하나인 DNS 는 도메인 이름과 IP 주소를 상호 매핑하는 분산 데이터베이스입니다.

1. 다음과 같이 탐색 표시줄에서 “네트워크 > DNS”를 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
DNS State	DNS 스위치
DNS Default Name	DNS 기본 이름을 입력하세요.

2. DNS 서버를 구성하려면 "추가"하세요.

3. “적용”하고 다음과 같이 마무리합니다.

4.2 시스템 시간

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

1. 다음과 같이 탐색 표시줄에서 “Network > System Time”을 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Time Source	SNTP, PC 또는 수동 모드에서 시간 소스를 선택하세요.
Time Zone	시간대 설정
Address Type	호스트 이름 또는 IPv4 주소(SNTP 로 설정된 시간 소스 포함)
Server Address	서버 주소(SNTP 에 의해 설정된 시간 소스 포함)
Server Port No.	서버 포트 번호(SNTP 에서 설정된 시간 소스 포함)
Date	날짜 정보: DD/MM/YYYY(수동 모드에서 시간 소스 설정)
Time	시간 정보: SS/MM/HH(시간 소스가 수동 모드로 설정된 경우)
Type	일광 절약 시간제 유형은 없음, 주기적, 비주기적, 미국 및 유럽으로 구분됩니다.

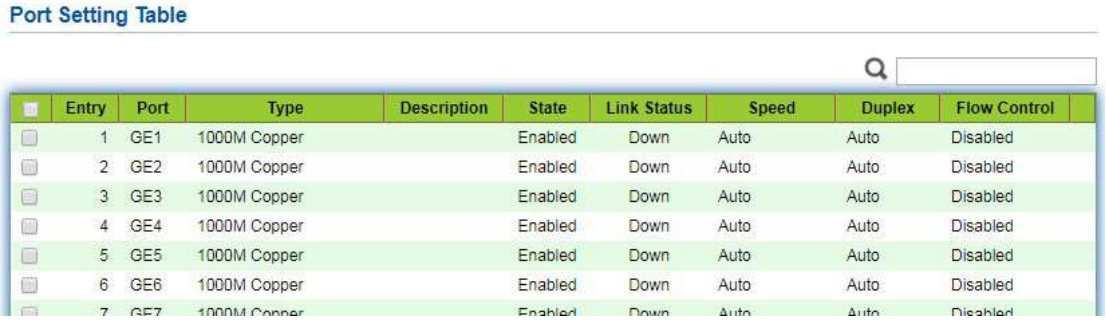
Reimbursed Time	일광 절약 시간제 환급 시간
Cyclic Mode	일광 절약 시간의 순환 모드 구성
Non-cyclic Mode	일광 절약 시간제의 비순환 모드 구성

5 포트

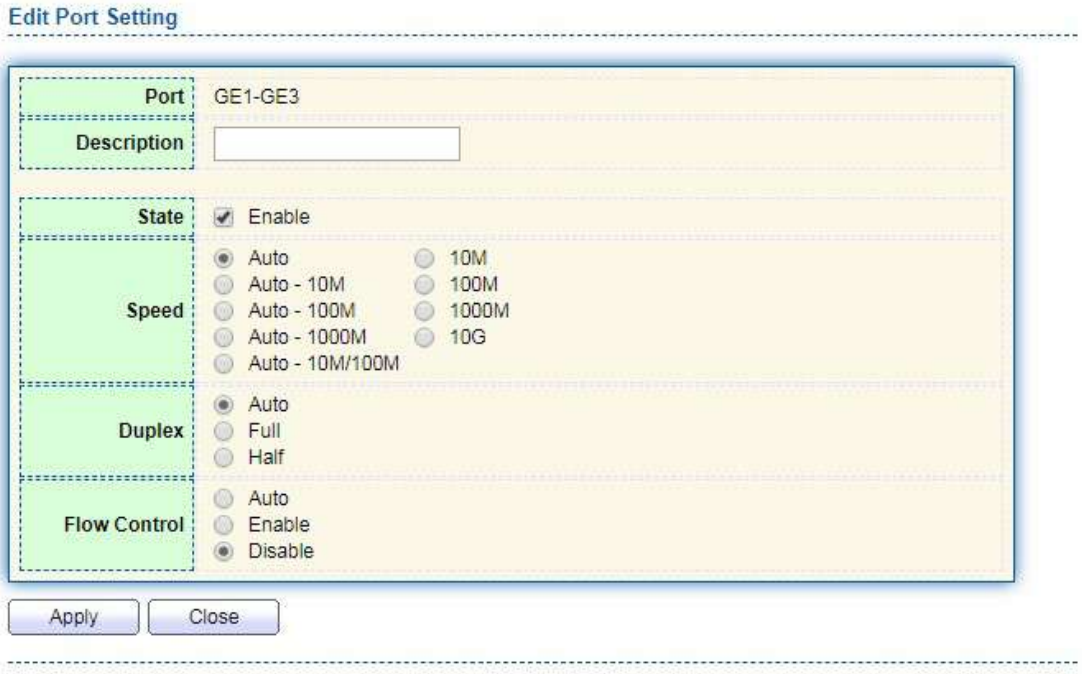
5.1 포트 설정

사용자가 원하는 대로 이더넷 인터페이스를 조회하고 구성할 수 있도록 인터페이스를 식별해야 합니다.

1. 탐색 표시줄에서 " Port > Port Setting "을 클릭합니다.



2. 구성할 포트를 선택하고 다음과 같이 "편집"합니다.



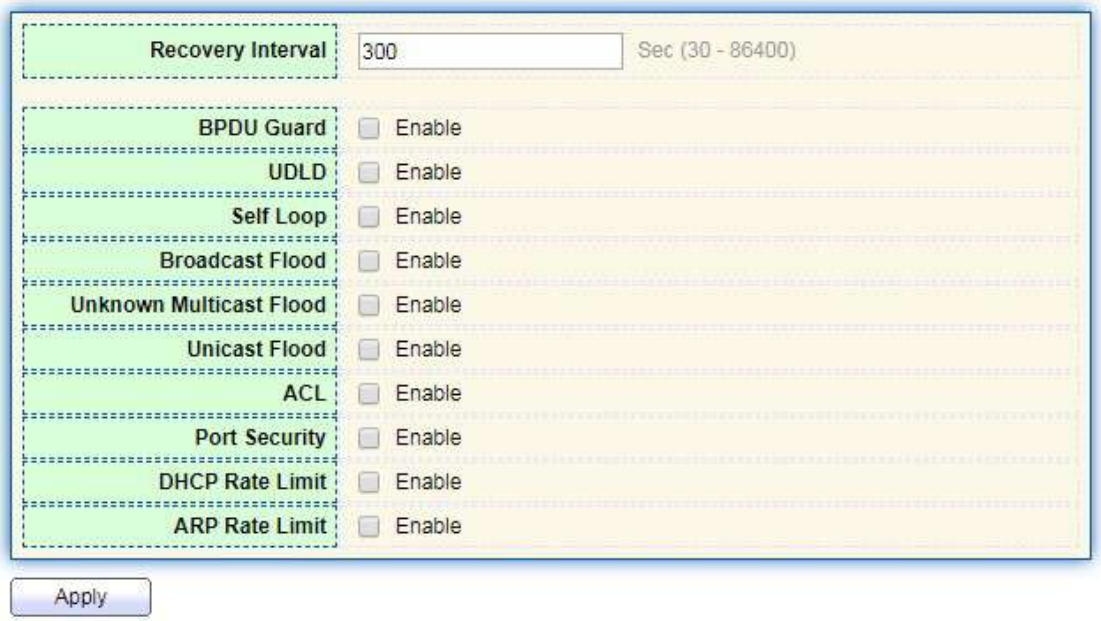
인터페이스 데이터는 다음과 같습니다

설정 항목	설명
Port	포트 목록
Description	포트 별칭
State	포트 활성화 또는 비활성화
Speed	필수 10Mb, 100Mb 및 1,000Mb 상태로 구성 가능한 자동 협상. 10Mbit/s, 100Mbit/s 및 1,000Mbit/s 를 포함한 인터페이스 속도는 이더넷 전기 인터페이스에 사용할 수 있으며 필요에 따라 선택 사항입니다.
Duplex	전이중 또는 반이중으로 구성 가능한 자동 협상.
Flow Control	로컬 네트워크와 상대 네트워크 장치 모두에서 활성화되면 로컬 네트워크는 네트워크 정체가 있을 때 메시지 전송을 중지하도록 다른 네트워크 장치에 알립니다. 반대쪽에서는 메시지 손실이 전혀 발생하지 않도록 일시적으로 명령을 실행합니다. 비활성화 - PAUSE 프레임 수신 및 전송이 비활성화됩니다. PAUSE 프레임의 수신 및 전송을 활성화합니다. 자동 협상 - 상대 네트워크 장치와 PAUSE 프레임을 자동으로 협상합니다.

5.2 오류 비활성화

일반적으로 스위치의 소프트웨어가 포트에서 일부 오류를 감지하면 포트가 즉시 닫힙니다. 즉, 스위치 운영 체제가 스위치 포트에서 일부 오류 이벤트를 감지하면 스위치는 자동으로 포트를 닫습니다.

1. 탐색 모음에서 " Port > Error Disabled "를 클릭하여 다음과 같이 구성을 활성화하거나 비활성화합니다.



5.3 Link Aggregation

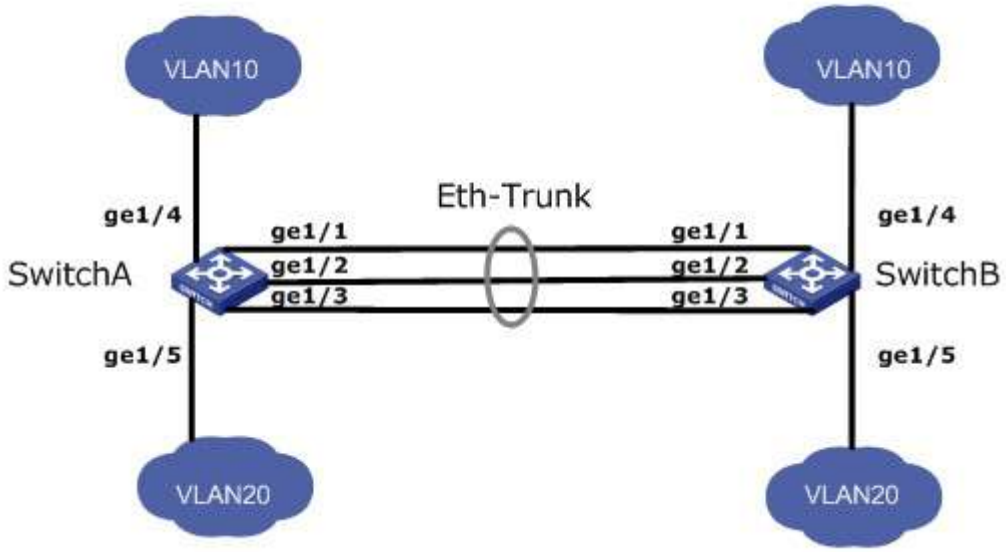
Link Aggregation 은 물리적 인터페이스 그룹을 단일 논리적 인터페이스로 묶어 대역폭과 안정성을 확장합니다.

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

끊임없이 확장되는 네트워크 크기는 링크 대역폭과 안정성에 대한 사용자의 요구를 증가시킵니다. 전통적으로 대역폭을 최적화하기 위해 고속 인터페이스 보드나 호환 장비를 교체하는 경우가 많았는데, 이는 비용이 많이 들고 유연성이 떨어졌습니다.

Link Aggregation Technology 는 하드웨어를 업그레이드하지 않고도 여러 물리적 인터페이스를 단일 논리적 인터페이스로 묶습니다. 백업 메커니즘은 안정성을 향상시킬 뿐만 아니라 다양한 물리적 링크에서 흐름 로드를 공유합니다.

아래에 표시된 것처럼 스위치 A 는 Eth-Trunk 논리적 링크로 묶인 3 개의 이더넷 링크를 통해 스위치 B 와 연결됩니다. 대역폭은 총 3 개 링크의 대역폭과 동일하므로 대역폭이 넓어집니다. 한편, 이 세 가지 링크는 상호 백업되어 더욱 안정적입니다.



링크 집계는 다음 요구 사항을 충족할 수 있습니다.

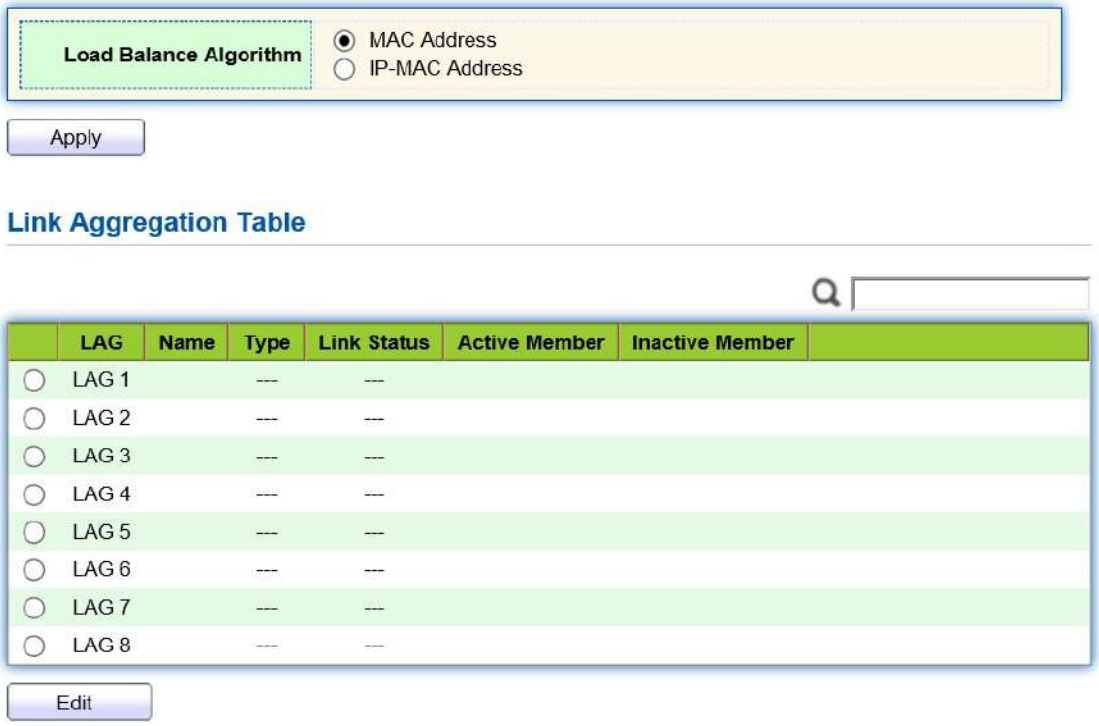
- 하나의 링크에 연결된 두 개의 스위치의 대역폭이 부족합니다.
- 하나의 링크에 연결된 두 개의 스위치에 대한 신뢰성이 부족합니다.

Link Aggregation 은 LACP(Link Aggregation Control Protocol) 상태에 따라 수동 모드와 LACP 모드로 구분됩니다.

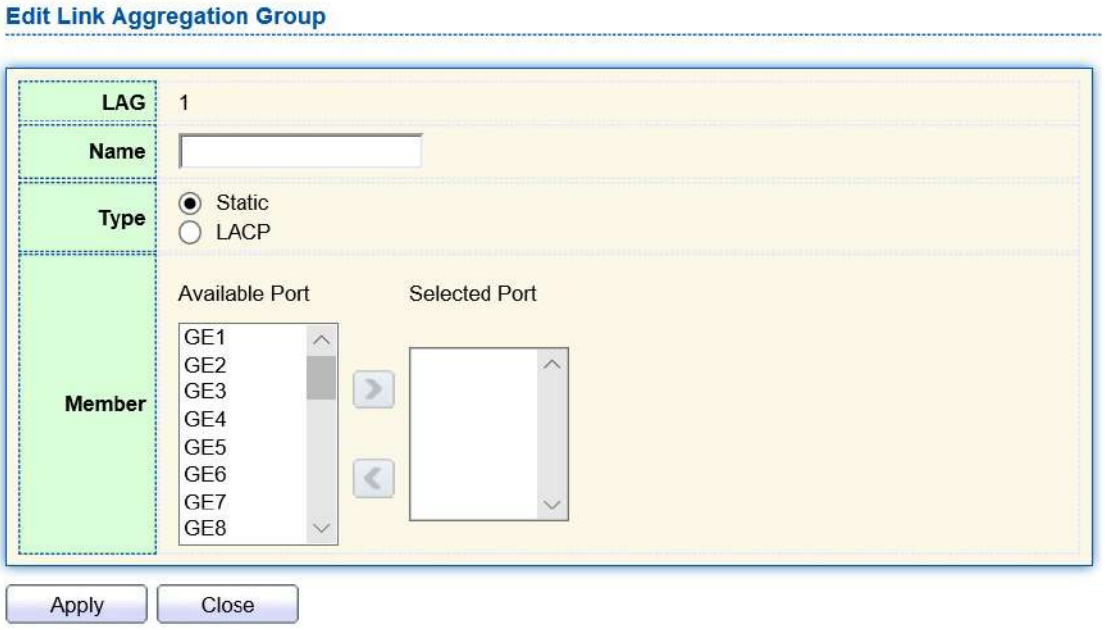
첫 번째 모드인 Eth-Trunk 설정에서는 LACP 없이 멤버 인터페이스 액세스를 수동으로 추가해야 합니다. 모든 링크가 데이터 전달 및 로드 공유에 포함되므로 로드 공유 모드라고도 합니다. 활성 링크에 장애가 발생하는 경우 LAG 는 나머지 링크의 평균 부하를 계산합니다. 이 모드는 직접 연결된 두 장치에 더 큰 링크 대역폭이 필요하지만 LACP 에 액세스할 수 없는 상황에서 선호됩니다.

5.3.1 그룹

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



2. 사용 가능한 8 개의 LAG 중 하나를 선택하고 다음과 같이 구성 페이지를 "편집"합니다.

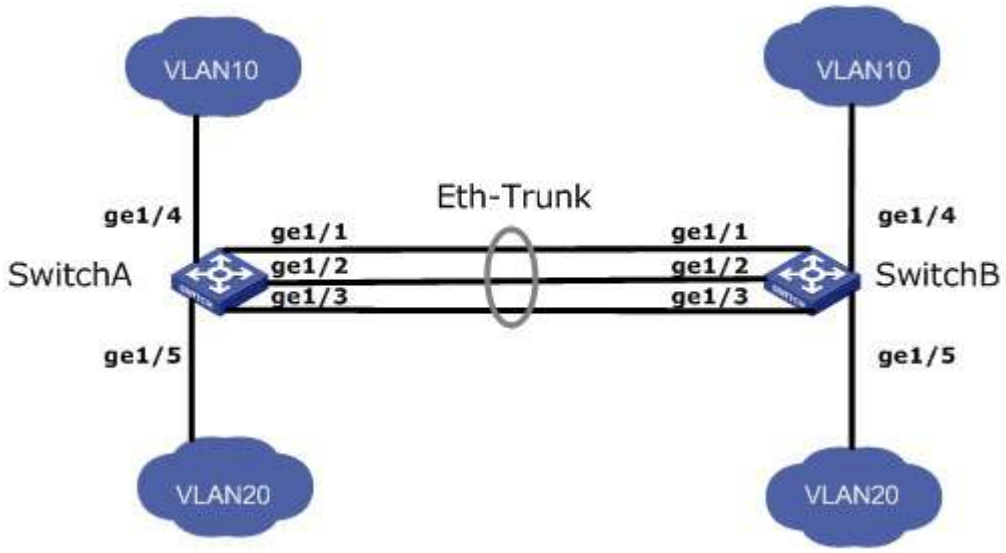


인터페이스 데이터는 다음과 같습니다

설정 항목	설명
LAG	1 부터 8 까지 번호가 매겨진 8 개의 LAG 가 있습니다.
Name	필요에 따라 수정할 수 있는 LAG 에 대한 설명입니다.

Type	수동 모드와 LACP 모드 중에서 선택합니다.
Member	LAG 에서는 최대 8 개의 멤버 포트를 사용할 수 있습니다.

아래 그림과 같이 스위치 A 와 스위치 B 는 각각 이더넷을 통해 VLAN 10 과 20 을 연결하며, 이들 사이에는 대규모 데이터 흐름이 있습니다.
스위치 A 와 B 모두 VLAN 통신을 위한 우수한 링크 대역폭을 제공할 것으로 예상됩니다. 한편, 안정적인 데이터 전송과 링크를 위해서는 중복성이 있어야 합니다.
수동 모드의 네트워킹 다이어그램 LAG

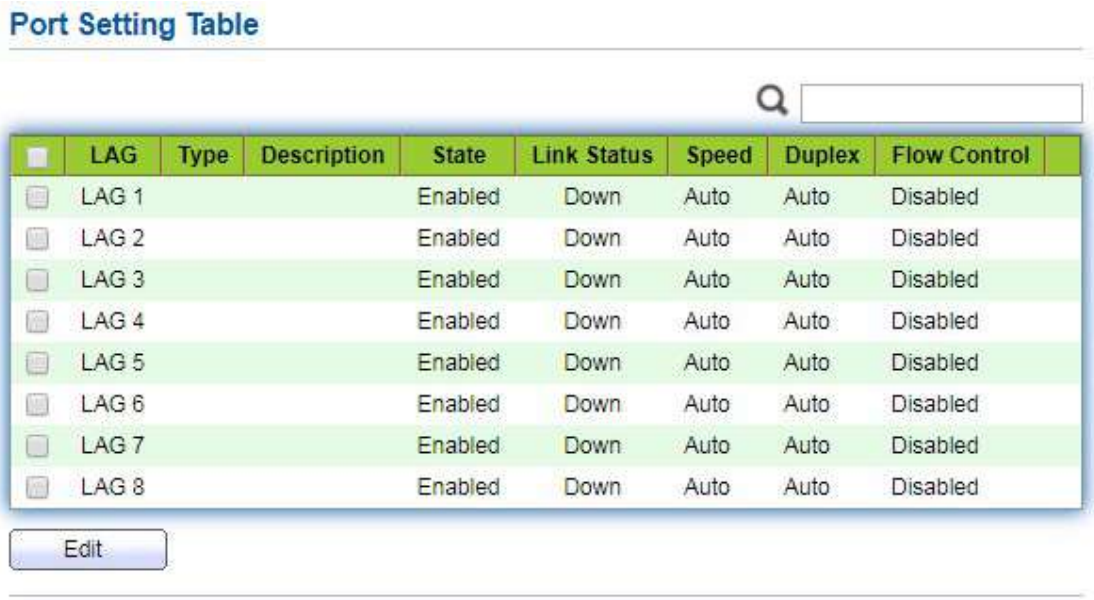


1. SwitchA 에서 ETH 트렁크 인터페이스를 생성하고 멤버 인터페이스를 추가하여 링크 대역폭을 늘립니다. SwitchB 의 구성은 SwitchA 의 구성과 유사합니다. “포트 > 링크 집합 > 그룹”을 클릭하고 “LAG 1”과 포트 GE1, 2, 3 을 선택한 후 오른쪽에서 선택한 포트로 이동합니다. “적용”하고 다음과 같이 마무리합니다.

5.3.2 포트 설정

Aggregation Group 멤버 포트의 속성 구성

1. “Port > Link Aggregation > Port Setting”을 클릭하면 다음과 같이 집합 그룹 구성원 포트의 속성 구성 인터페이스로 들어갑니다.



5.3.3 LACP

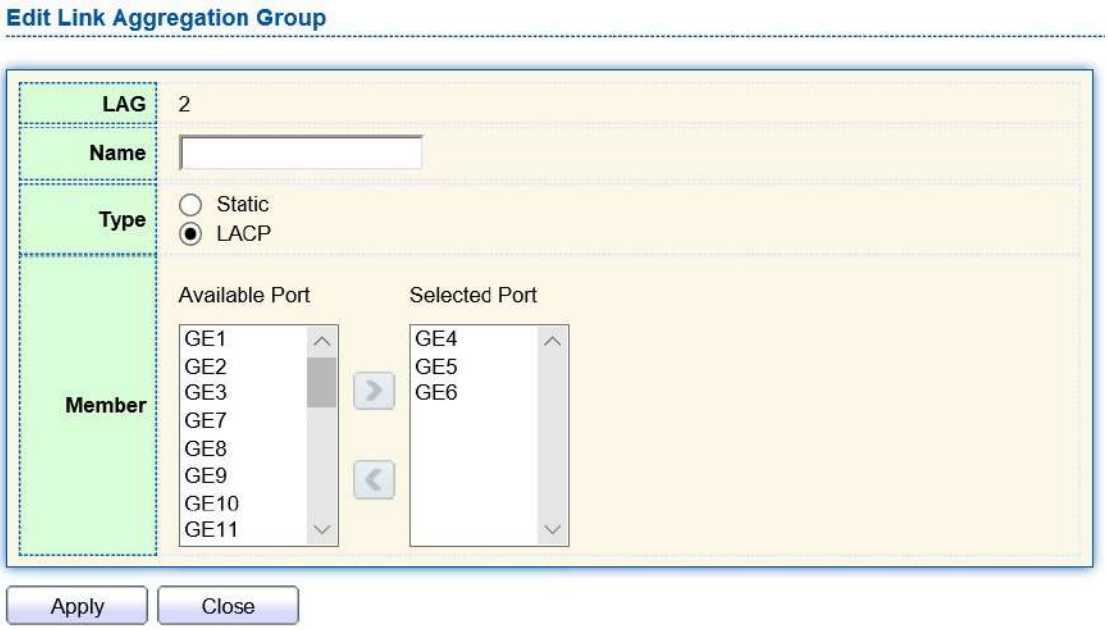
IEEE 802.3ad 표준을 기반으로 하는 LACP(Link Aggregation Control Protocol)는 링크를 동적으로 집계 및 분리합니다. LACPDU(Link Aggregation Control Protocol Data Unit)를 통해 상대 네트워크 기기와 정보를 교환합니다.

포트가 LACP 를 사용한 후 LACPDU 를 전송하여 시스템 우선순위, 시스템 MAC, 포트 우선순위 및 번호, 작동 키를 상대 네트워크 장치에 알려줍니다. 반대 장치는 해당 정보를 수신한 후 다른 포트에 저장된 정보와 비교하여 동적 집계에 대한 포트 참여 또는 종료에 대한 합의에 도달합니다.

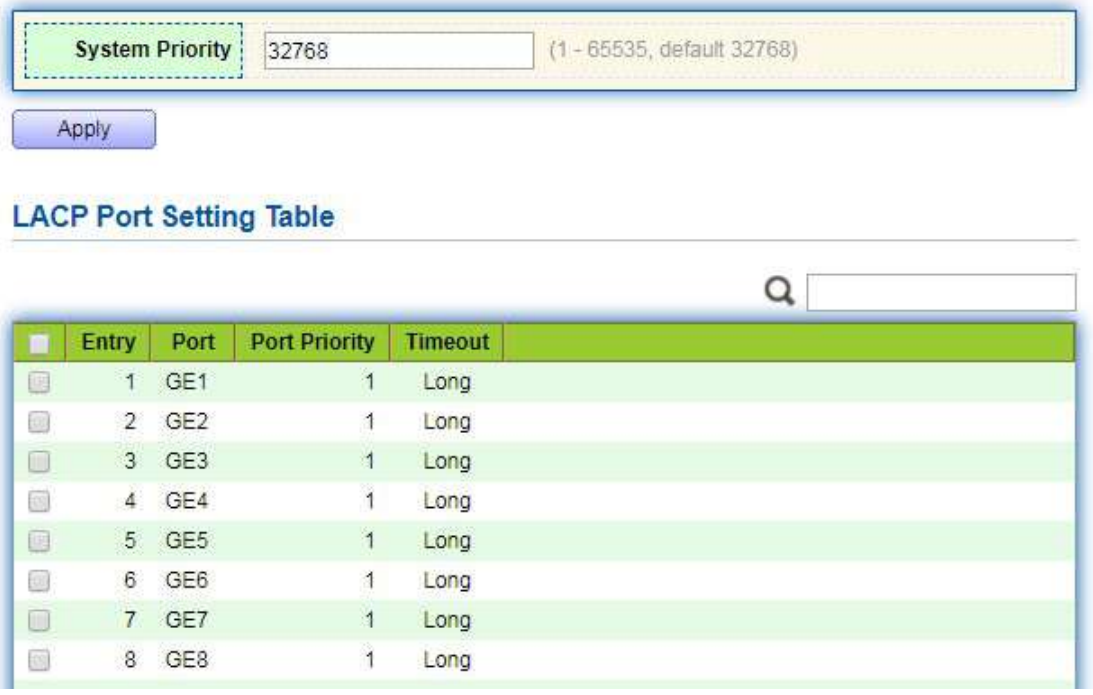
동적 LACP 통합은 시스템에 의해 자동으로 생성되거나 삭제됩니다. 즉, 내부 포트가 자체적으로 추가되거나 제거될 수 있습니다. 동일한 속도, 이중 및 기본 구성을 사용하여 동일한 장치에 연결된 포트만 집계할 수 있습니다.

동적 링크 통합 추가 가이드:

1. 탐색 모음에서 " Port > Link Aggregation > Group "을 클릭하고 LAG ID 및 LACP 모드를 선택한 후 다음과 같이 "편집"합니다.



2. 탐색 표시줄에서 "포트 > 링크 집합 > LACP"를 클릭하여 시스템 우선 순위, 포트 우선 순위, 시간 초과 방법과 같은 LACP 속성을 다음과 같이 구성합니다.



인터페이스 데이터는 다음과 같습니다

설정 항목	설명
System Priority	LACP 는 우선순위 표준에 따라 두 장치 간의 활성 및 수동 모드를 결정합니다.
Port	포트 목록

Port Priority	LACP 는 상위 시스템의 포트 우선순위에 따라 동적 LAG 구성원 모드를 결정합니다.
Timeout	LACP 메시지의 전송 빈도를 결정합니다.

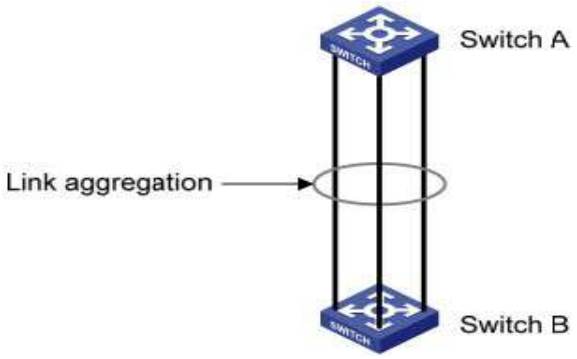
:

작업 패턴을 변경하기 전에 Eth-Trunk 에 액세스하는 멤버 인터페이스가 없는지 확인하십시오. 그렇지 않으면 실패합니다.

로컬 네트워크 장치의 작업 패턴은 반대 네트워크 장치의 작업 패턴과 일치해야 합니다.

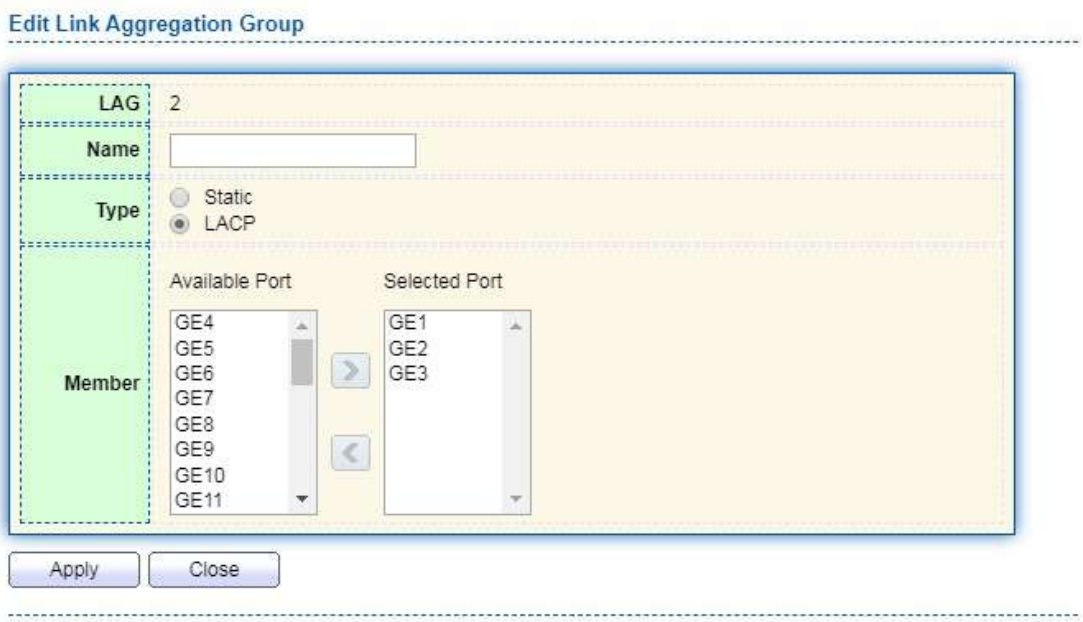
이더넷 스위치 A 는 각 구성원 포트별로 부하를 공유하기 위해 GE1 에서 GE3, 스위치 B 까지 3 개의 포트를 통합합니다.

다음 구성은 동적 집계를 통해 예시됩니다.



다음은 스위치 A 만의 구성이며, 포트 집합을 위해 스위치 B 의 구성과 동일하게 유지되어야 합니다.

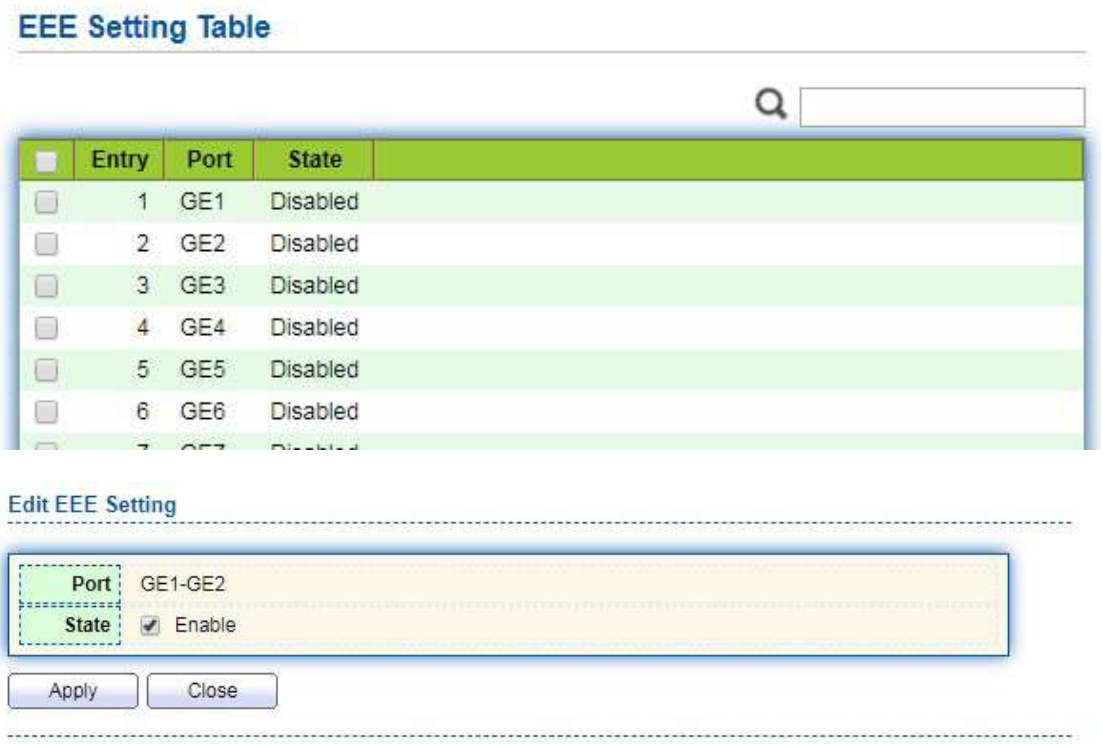
1. 탐색 모음에서 "포트 > 링크 집계 > 그룹"을 클릭하고 LAG 2 로 "편집"을 클릭한 다음 LACP 모드에서 GE1-GE3 을 선택합니다. "적용"하고 다음과 같이 완료합니다.



5.4 EEE

유량이 0 이하인 경우 포트 전원이 꺼집니다.

1. 탐색 표시줄에서 " Port > EEE "를 클릭하고 포트를 선택한 다음 "편집"을 선택하여 다음과 같이 구성 인터페이스로 들어갑니다.

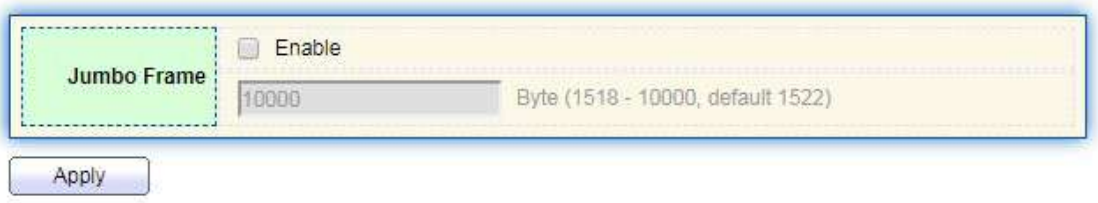


2. 포트 활성화 태그를 설정하고 "적용"하면 다음과 같이 구성이 완료됩니다.

5.5 점보 프레임

포트의 MTU(최대 전송 단위)를 설정합니다.

1. 탐색 모음에서 " Port > Jumbo Frame "을 클릭하고 다음과 같이 점보 프레임 구성 인터페이스로 들어갑니다.

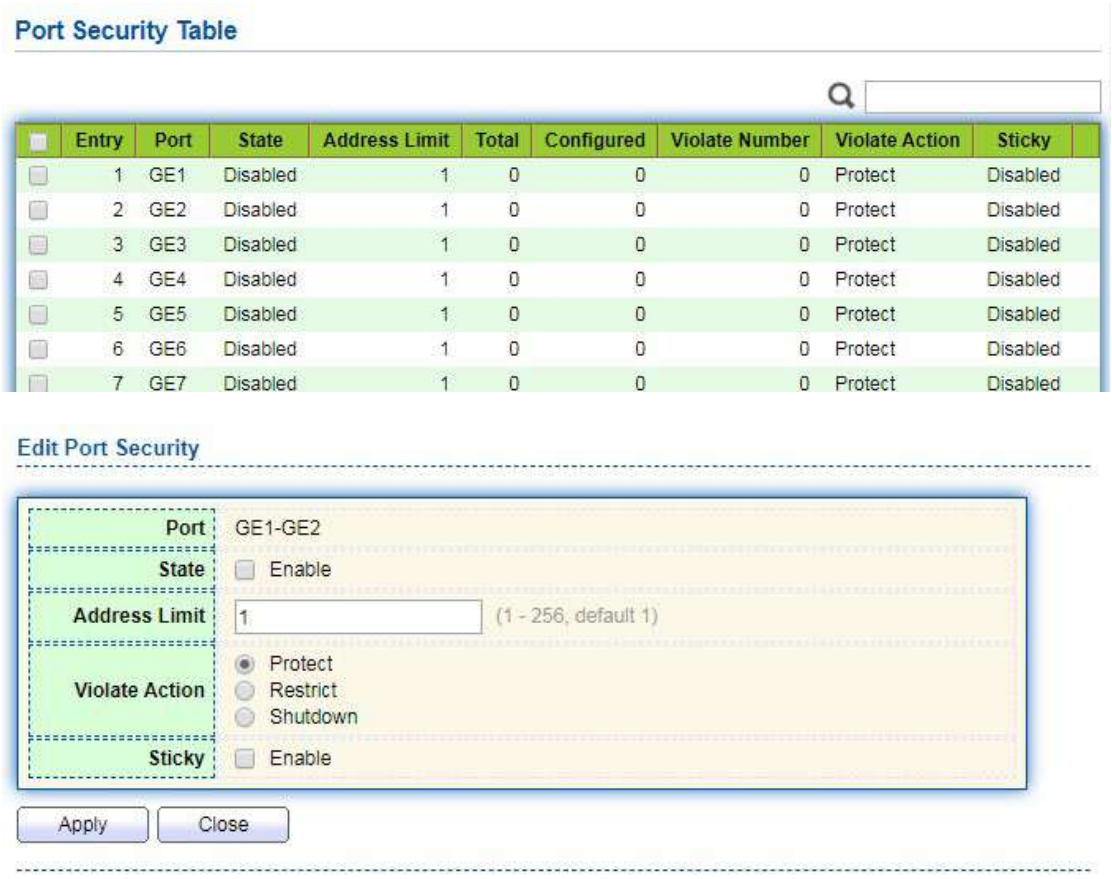


5.6 포트 보안

포트 보안 기능은 MAC 주소 테이블을 통해 스위치 포트에 연결된 이더넷 MAC 주소를 기록하며, 이 포트를 통해 하나의 MAC 주소만 통신할 수 있습니다. 다른 MAC 주소에서 보낸 패킷이 이 포트를 통과하면 포트 보안 기능이 이를 방지합니다. 포트 보안 기능을 사용하면 승인되지 않은 장치가 네트워크에 액세스하는 것을 방지하고 보안을 강화할 수 있습니다. 또한 포트 보안 기능을 사용하여 MAC 주소 플러딩으로 인해 MAC 주소 테이블이 가득 차는 것을 방지할 수도 있습니다.

1. 탐색 표시줄에서 " Port > Port Security "을 클릭하고 다음과 같이 포트 보안 구성 인터페이스로 들어갑니다.

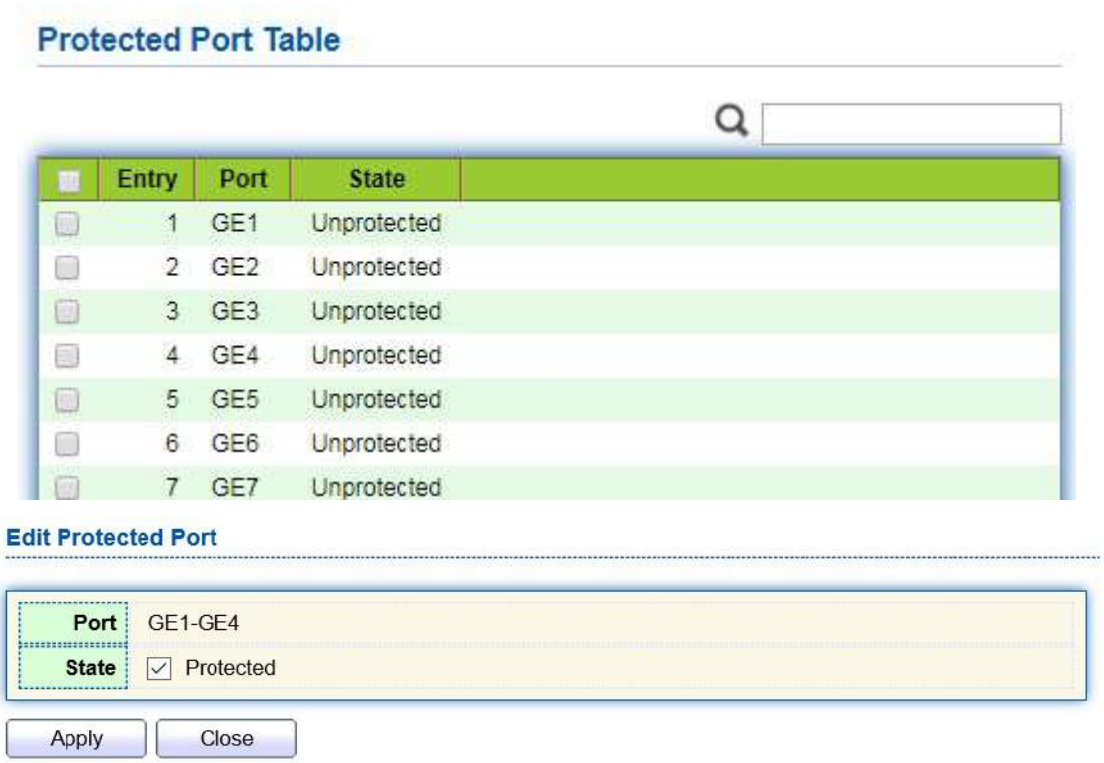
2. 탐색 모음에서 "포트 > 포트 보안"을 클릭하고 포트를 선택한 다음 "편집"을 선택하여 다음과 같이 포트 수준 구성 인터페이스로 들어갑니다.



5.7 보호된 포트

때로는 흐름에 상호 통신이 필요하지 않더라도 브로드캐스트, 멀티캐스트 등의 메시지가 각 포트에서 플러딩됩니다. 이러한 상황에서는 포트 격리를 통해 두 포트 간의 메시지를 분리할 수 있습니다.

1. 탐색 모음에서 " Port > Protected Port "를 클릭하고 격리할 포트를 선택한 후 "편집"을 클릭하여 이 기능을 다음과 같이 전환합니다.



포트 격리를 달성하기 위한 가이드:
1. 탐색 바에서 “Port > Protected Port”를 클릭하고 격리할 GE1, 2, 3 을 선택하고 “편집”합니다. "적용"하고 다음과 같이 완료합니다.

2. GE1, 2, 3 은 다른 비격리 포트처럼 상호 통신에 실패합니다.

5.8 스톰 컨트롤

브로드캐스트, 알 수 없는 멀티캐스트, 유니캐스트 메시지를 통해 발생하는 Storm 은 다음과 같이 방지됩니다. 이러한 메시지는 각각 패킷 속도에 따라 표시되지 않습니다. 모니터링 인터페이스에서 수신된 메시지의 평균 속도는 검사 간격 동안 구성된 최대 임계값과 비교됩니다. 평균 비율이 최대 임계값을

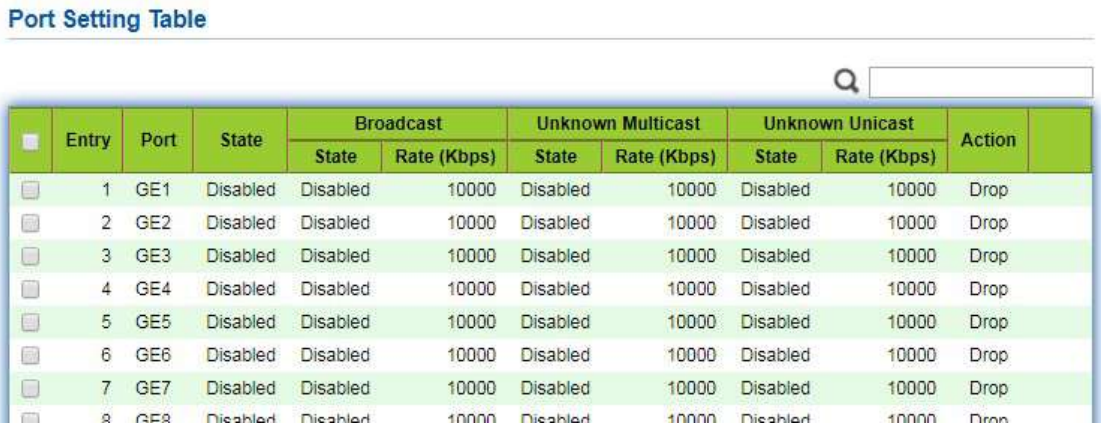
초과하는 경우 구성된 폭풍 정책이 이 인터페이스에서 수행됩니다.

L2 이더넷 인터페이스가 브로드캐스트, 알 수 없는 멀티캐스트 또는 유니캐스트 메시지를 수신할 때 대상 MAC 주소에 따라 송신 인터페이스를 인식할 수 없는 경우 장치는 해당 메시지를 동일한 VLAN(Virtual Local Area Network)에 있는 다른 L2 인터페이스로 전달합니다. 결과적으로 브로드캐스트 스톰(Broadcast Storm)이 발생하여 기기 동작 성능이 저하될 수 있습니다.

방송 폭풍을 피하기 위해 폭풍 치안 특성을 통해 세 가지 종류의 메시지 흐름을 제어할 수 있습니다.

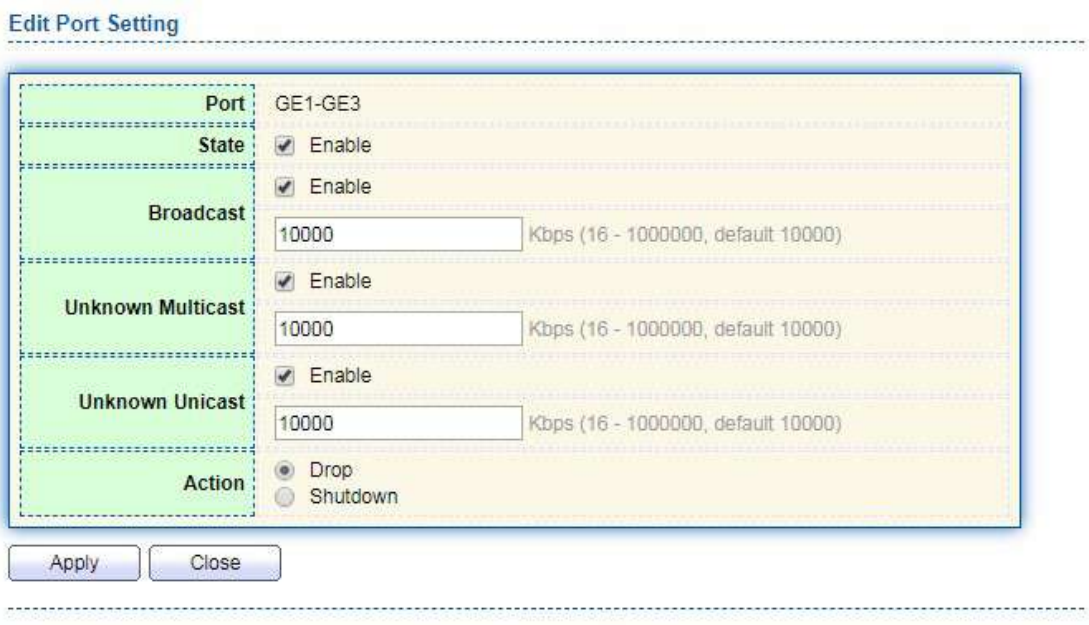
1. 네비게이션 바에서 “Port > Storm Control”를 클릭하면 모드 등 스톰 폴리싱과 관련된 속성을 다음과 같이 구성할 수 있습니다.

2. 적절한 포트를 선택하고 각 포트에서 브로드캐스트, 알 수 없는 멀티캐스트 및 유니캐스트 스톰의 정책 속도를 구성하여 "편집"합니다.



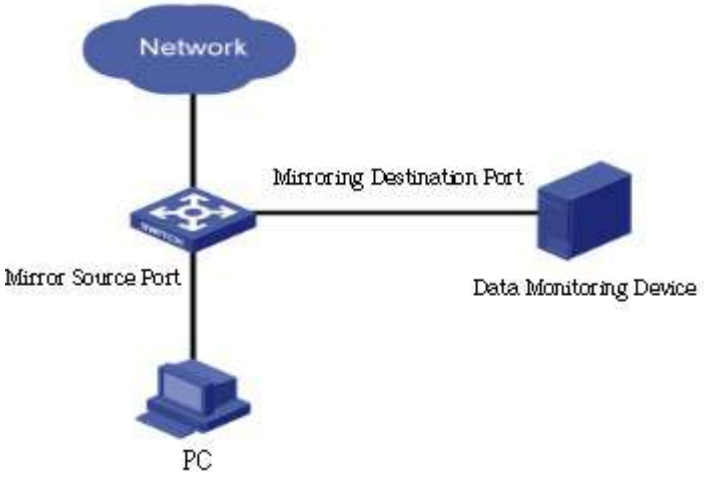
Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

3. 폭풍 스위치 및 속도 등의 정보를 구성하고 “적용”하고 다음과 같이 완료합니다.



5.9 미러링

포트 미러링은 지정된 스위치 포트의 메시지를 대상 포트로 복사합니다. 복사된 포트가 Source Port, 복사되는 포트가 Destination Port 가 됩니다. 대상 포트는 데이터 검사 장치에 액세스하여 사용자가 수신된 메시지를 분석하여 네트워크를 모니터링하고 다음과 같이 문제를 해결할 수 있도록 합니다.



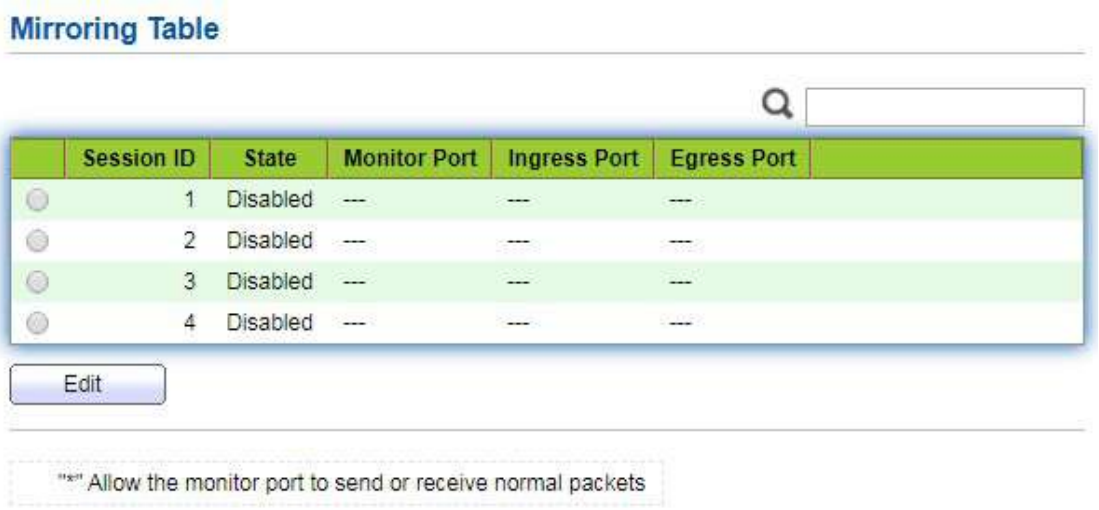
Instance

PC1 과 PC2 는 각각 인터페이스 GE1 과 GE2 를 통해 스위치 A 에 액세스합니다.

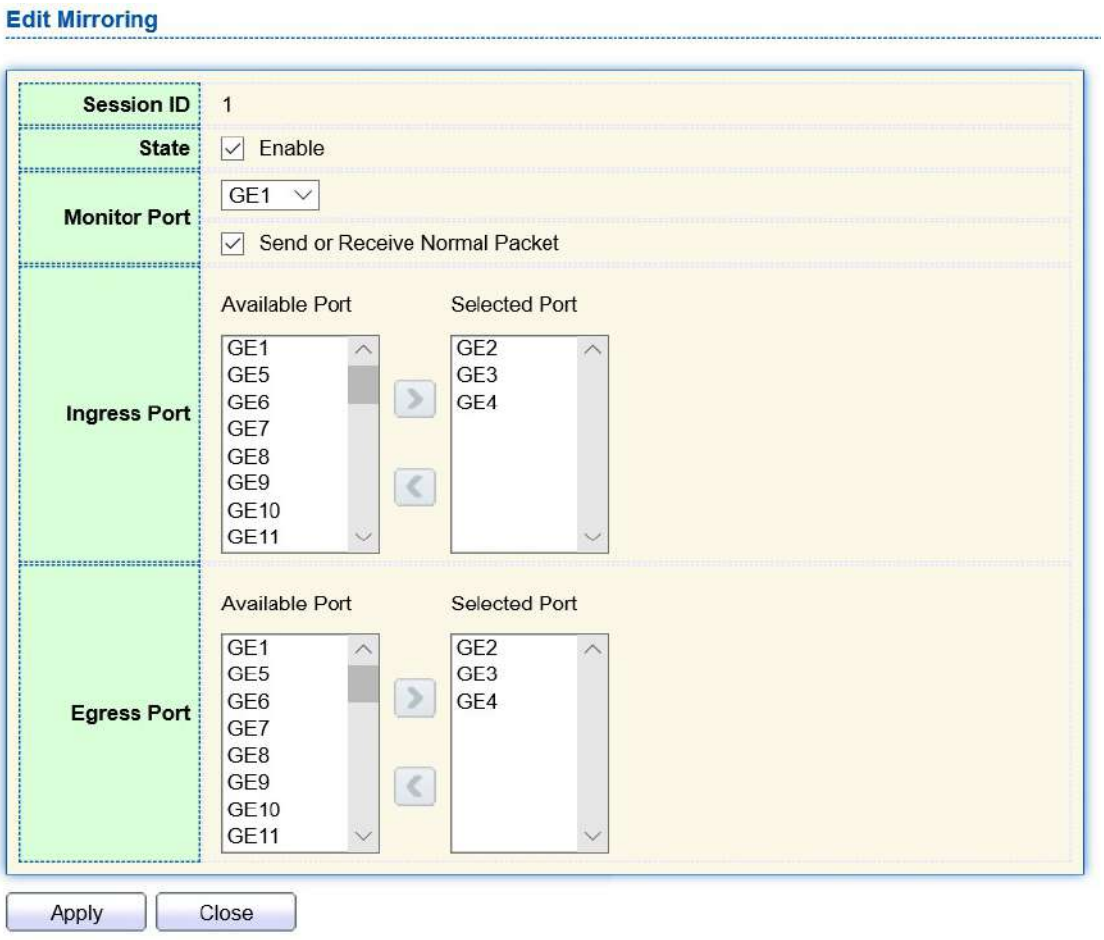
사용자는 PC2 에서 PC1 로 전송되는 메시지를 모니터링하려고 합니다.

1. 탐색 표시줄에서 “Port > Mirroring”을 클릭하세요. 4 개 세트의 흐름 미러링

규칙을 다음과 같이 구성할 수 있습니다.



2. 하나의 세션을 선택하고 미러링 그룹 구성 인터페이스에서 "편집"합니다.



인터페이스 데이터는 다음과 같습니다

설정 항목	설명

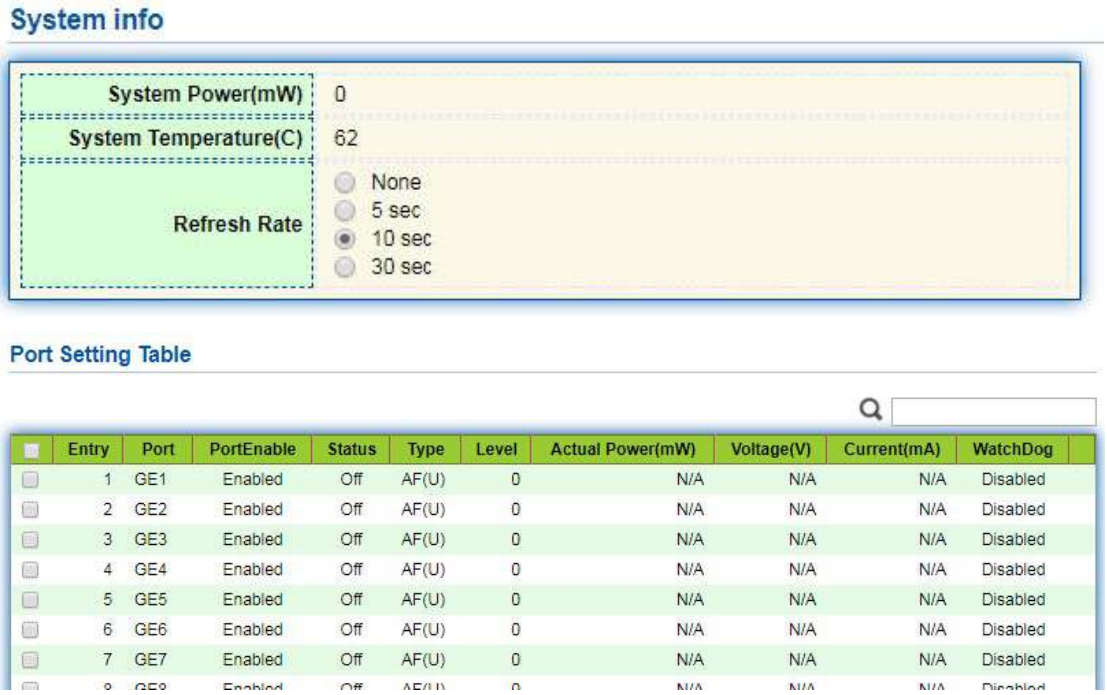
Session ID	스위치에는 기본적으로 4 개의 세션 ID 가 있습니다.
State	미러링 그룹을 활성화하거나 비활성화할 수 있습니다.
Monitor Port	Link Aggregation 포트와 소스 포트를 제외하고 일반 물리적 포트는 하나만 선택할 수 있습니다.
Ingress Port	수신된 모든 메시지는 대상 포트로 미러링됩니다.
Egress Port	전송된 모든 메시지는 대상 포트로 미러링됩니다.

6 POE 설정

PoE(Power over Ethernet)는 IP 기반의 단말(예: IP 전화, WAP, IP 카메라)에 데이터 신호를 전송하고 기존 Cat-5 네트워크 케이블 연결 상태를 변경하지 않고 장치에 직류를 공급합니다. 안전한 구조의 케이블링과 정상적인 네트워크 운영을 보장하여 비용을 최소화합니다.

6.1 PoE 포트 설정

1. 다음과 같이 탐색 표시줄에서 “POE Setting > POE Port Setting”을 클릭합니다.



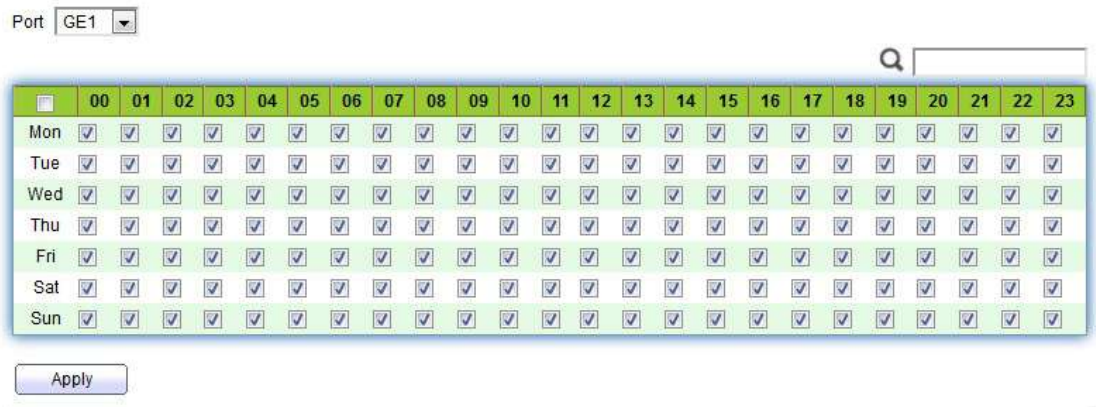
2. 구성할 포트를 선택하고 다음과 같이 "편집"합니다.

인터페이스 데이터는 다음과 같습니다

설정 항목	설명
PortEnable	Poe 포트 전원 활성화/비활성화
WatchDog	Poe 포트 감시 기능 활성화/비활성화; 워치독 기능을 활성화한 후 POE 포트에 지속적으로 전원이 공급되지만 트래픽이 없으면 POE 워치독이 트리거됩니다. 감지 후 2 분 후에 전원 공급이 중단된 후 전원이 켜집니다. 총 감지 주기는 5 회입니다.

6.2 POE 포트 타이머 설정

1. “POE Setting > POE Port Timer Setting”을 클릭하고 Poe 스케줄의 전원 공급 시간을 선택합니다. “적용”하고 다음과 같이 마무리합니다.



6.3 POE 포트 타이머 재부팅 설정

설정에 따라 포트에 따라 주기적으로 전원 공급을 다시 시작할 수 있습니다.

1. 다음과 같이 탐색 표시줄에서 “POE Setting > POE Port Timer Reboot Setting”을 클릭합니다.

2. 포트를 선택하고 "편집"을 선택하여 구성 인터페이스로 들어갑니다.

인터페이스 데이터는 다음과 같습니다

설정 항목	설명
Port	포트 목록
RebootTimer	PoE 포트가 PoE 전원 공급을 끄는 시간 동기화 시간을 설정합니다. 분 단위로만 설정이 지원됩니다.
DelayTimer	재시작 시간에 PoE 전원 공급 장치가 꺼진 후 재시작 및 전원 공급 장치 켜기까지의 지연 시간은 분으로만 설정할 수 있습니다.

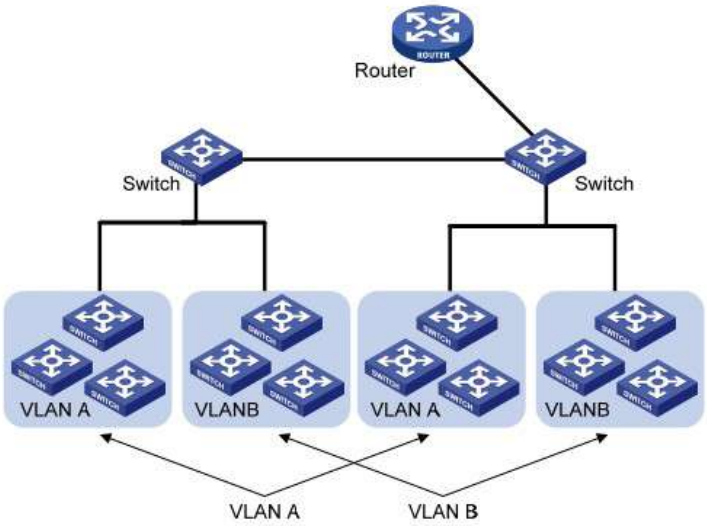
Note:

- 이 기능을 사용하려면 시스템 시간 동기화를 설정해야 합니다.
- PoE 포트 재시작의 최소 세분성 시간은 분입니다.
- 재시작 시간이 설정되면 지연 시간도 설정되어야 합니다.
- 지연 시간이 00:00:00 이면 해당 포트에 더 이상 전원이 들어오지 않는다는

의미입니다.

7 VLAN

VLAN 은 물리적 위치에 국한되지 않고 구성되므로 동일한 VLAN 에 있는 호스트를 마음대로 배치할 수 있습니다. 아래 그림과 같이 각 VLAN 은 브로드캐스트 도메인으로서 물리적 LAN 을 논리적 LAN 으로 구분합니다. 호스트는 전통적인 통신 방식으로 메시지를 교환할 수 있습니다. 서로 다른 VLAN 에 있는 호스트의 경우 라우터나 L3 스위치와 같은 장치가 필수입니다.



VLAN 은 다음과 같은 측면에서 기존 이더넷보다 우수합니다.

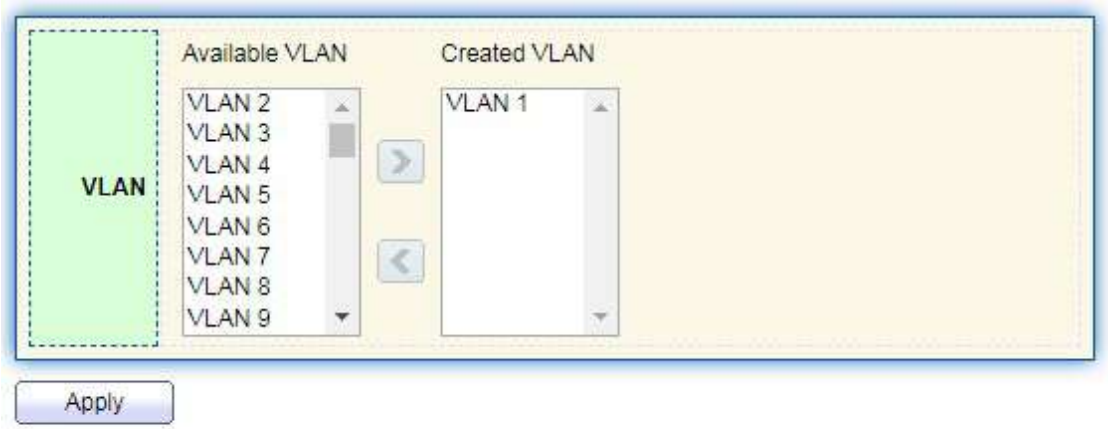
- 브로드캐스트 도메인 적용 범위: LAN 의 브로드캐스트 메시지는 대역폭을 절약하고 네트워크 관련 문제를 보다 효율적으로 처리하기 위해 VLAN 으로 제한됩니다.
- LAN 보안: VLAN 호스트는 데이터 링크 계층에서 메시지가 브로드캐스트 도메인으로 분리되어 있기 때문에 서로 통신할 수 없습니다. 레이어 3 전달을 위해서는 라우터나 레이어 3 스위치가 필요합니다.
- 가상 작업 팀 생성의 유연성: VLAN 은 물리적 네트워크의 제어를 넘어 가상 작업 팀을 생성할 수 있습니다. 사용자는 물리적 위치가 범위 내에서 이동하는 경우 구성을 변경하지 않고도 네트워크에 액세스할 수 있습니다. 이 관리 스위치는 802.1Q, 프로토콜, MAC 및 포트를 기반으로 하는 VLAN 유형과 호환됩니다. 기본 구성의 경우 802.1Q VLAN 모드를 채택해야 합니다. 포트 VLAN 은 스위치의 인터페이스 번호에 따라 구분됩니다. 네트워크 관리자는 각 스위치 인터페이스에 서로 다른 PVID, 즉 포트 기본 VLAN 을 부여합니다. VLAN 태그가 없는 데이터 프레임이 PVID 가 있는 스위치 인터페이스로 유입되면 동일한 PVID 로 표시되거나 인터페이스에 PVID 가 있더라도 추가 태그가 제거됩니다.

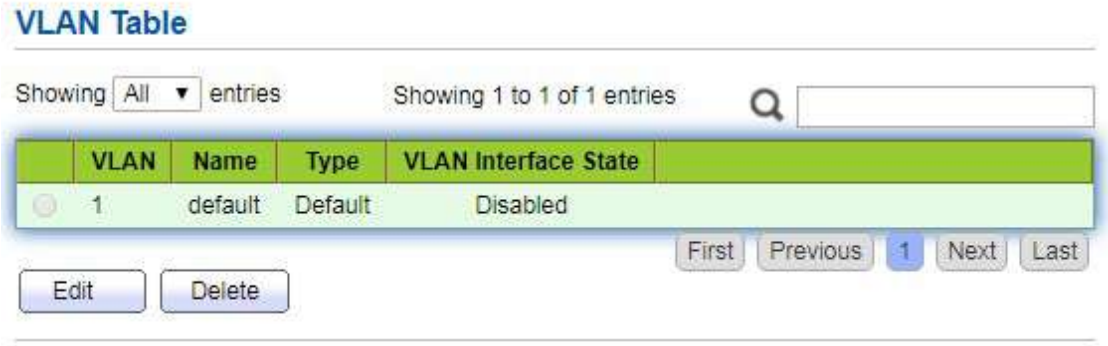
- VLAN 프레임에 대한 솔루션은 인터페이스 유형에 따라 달라지며, 이는 구성원 정의를 용이하게 하지만 구성원 이동성의 경우 VLAN 을 재구성합니다.

7.1 VLAN

7.1.1 VLAN 생성

1. “VLAN > VLAN > Create VLAN”을 클릭하여 유효한 VLAN 상자에서 이름을 선택하고 오른쪽의 VLAN 생성 상자로 이동합니다(최대 256 개의 VLAN 생성 가능). "적용"하고 다음과 같이 완료합니다.





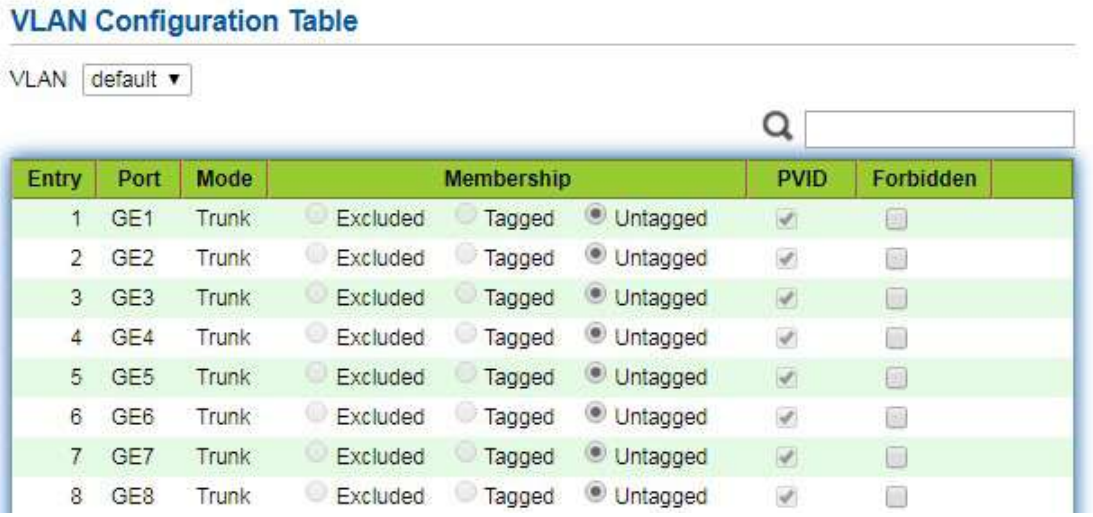
2. 생성된 VLAN 이 VLAN 테이블에 표시됩니다. 사용자는 다음과 같이 VLAN 을 "편집"할 수 있습니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN ID	1~4,094 범위의 ID를 선택해야 합니다. 예를 들어 1-3,5,7 및 9 입니다. LAN 1 이 기본값이며 다른 새 VLAN 에서 반복되지 않습니다.
Name	필요에 따라 VLAN 설명을 수정하는 것은 선택 사항입니다.

7.1.2 VLAN 구성

두 가지 방법이 있습니다. 하나는 단일 VLAN 아래에 여러 포트를 추가하는 것입니다. 다른 하나는 여러 VLAN 에 포트를 추가하는 것입니다. 다양한 목적에 따라 구성됩니다.
현재 포트를 지정된 VLAN 에 추가하는 첫 번째 방법에 대한 가이드입니다.
1. 네비게이션 바에서 “VLAN > VLAN > VLAN Configuration”을 클릭하고 왼쪽 상단의 VLAN ID 를 선택한 후 다음과 같이 포트 정보를 클릭합니다.



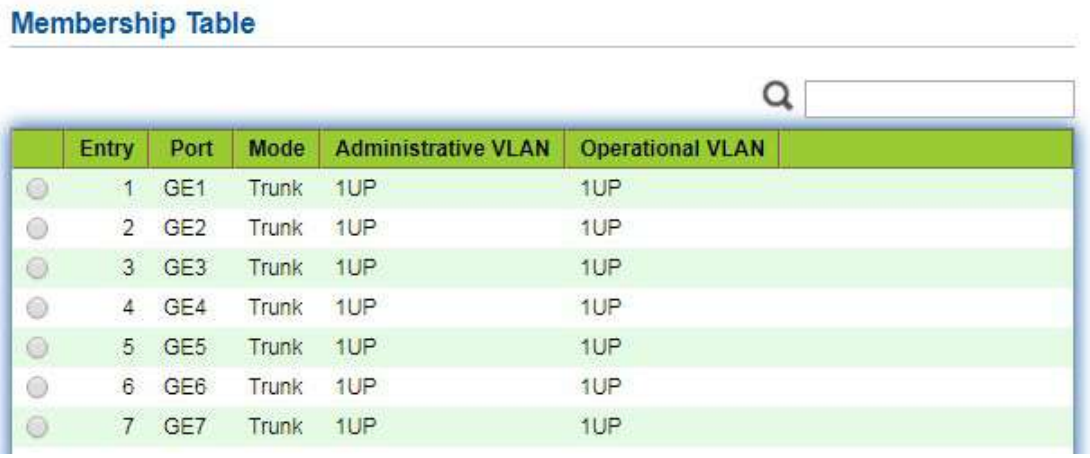
인터페이스 데이터는 다음과 같습니다.

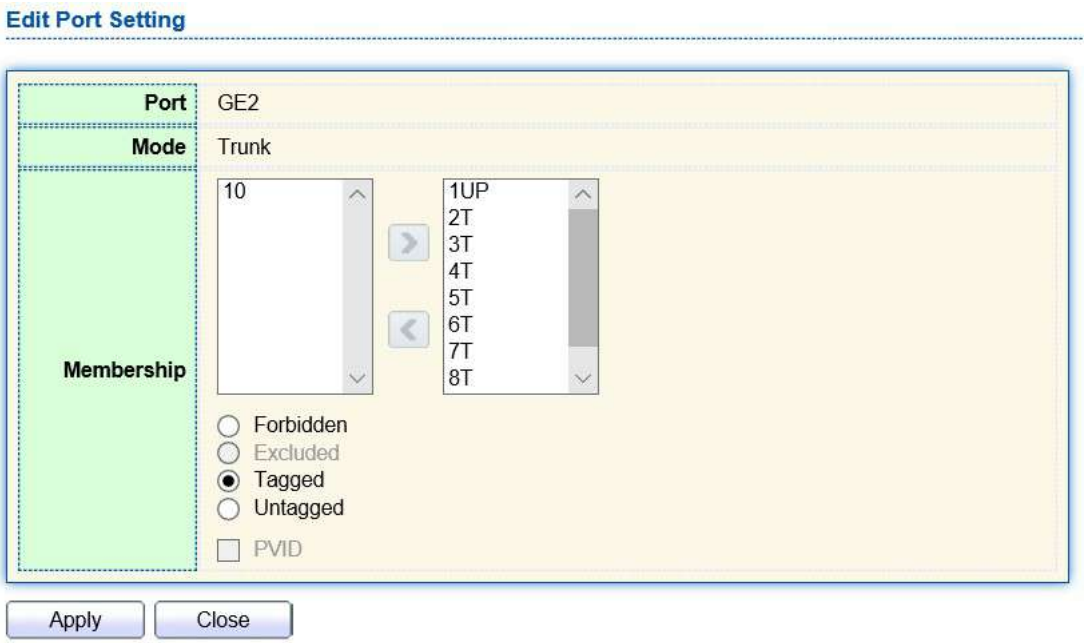
설정 항목	설명
VLAN	구성할 VLAN ID
Port	포트 목록

Mode	포트의 VLAN 모드
Membership	VLAN 포트의 구성원 역할: 제외됨: 포트가 이 VLAN 외부에 있습니다. 태그됨: 포트가 이 VLAN 의 태그된 멤버입니다. 태그 없음: 포트가 이 VLAN 의 태그가 없는 구성원입니다.
PVID	이 VLAN 이 포트 PVID 인지 여부
Forbidden	이 포트에서 VLAN 메시지 전달이 금지되는지 여부

7.1.3 맴버십

현재 포트를 지정된 VLAN 에 추가하는 두 번째 방법에 대한 가이드
1. 탐색 모음에서 "VLAN > VLAN > Membership"을 클릭하고 구성할 포트를 선택한 다음 "Edit"을 선택하여 해당 속성을 구성합니다.





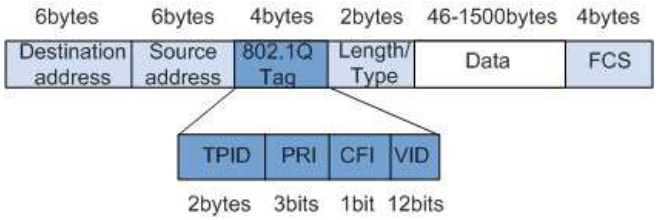
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
Mode	포트의 VLAN 모드
Membership	포트는 VLAN ID 및 VLAN 의 속성입니다. 금지됨: VLAN 메시지를 전달하지 마십시오. 제외됨: VLAN 외부의 포트 Tagged: VLAN 의 Tagged 멤버 태그 없음: VLAN 의 태그 없음 멤버 PVID: VLAN 이 포트 PVLAN 인지 여부

7.1.4 포트 설정

트렁크 구성. 다른 스위치와 연결되는 트렁크 인터페이스는 주로 트렁크 링크를 연결하여 VLAN 프레임이 흐르도록 합니다. IEEE 802.1q 는 트렁크 링크의 캡슐화 프로토콜이며 가상 브리지 LAN(Virtual Bridged Local Area Network)에 대한 공식 표준을 고려합니다. 소스 MAC 주소 필드와 프로토콜 필드 사이에 4 비트 802.1q 태그를 추가하여 이더넷의 프레임 형식을 변경합니다.

802.1q 프레임 형식



Meanings of 802.1q tag fields

필드	길이	이름	내용
TPID	2 bytes	프레임 유형을 설명하는 태그 프로토콜 식별자	값이 0x8,100 일 때의 802.1q Tag 프레임을 의미하며, 해당 장비가 이를 수신하지 못할 경우 폐기됩니다.
PRI	3 bits	프레임 우선순위	범위는 0 부터 7 까지이며, 우선 순위가 높을수록 더 큰 숫자로 표시됩니다. 스위치 혼잡 시 우선 순위가 높은 데이터 프레임이 우선적으로 전송됩니다.
CFI	1 bit	MAC 주소가 클래식 주소인지 여부를 나타내는 정식 형식 표시기입니다.	MAC 주소는 CFI 가 0 이면 클래식 주소이고 CFI 가 1 이면 비클래식 주소입니다. 이더넷과 토큰 링 간의 호환성을 촉진합니다. CFI 는 이더넷에서 0 이 됩니다.
VID	12 bits	VLAN ID 는 프레임이 속한 VLAN 을 나타냅니다.	범위는 0~4,095 이며, 0~4,095 는 프로토콜 보존 값이므로 1~4,094 까지 유효합니다.

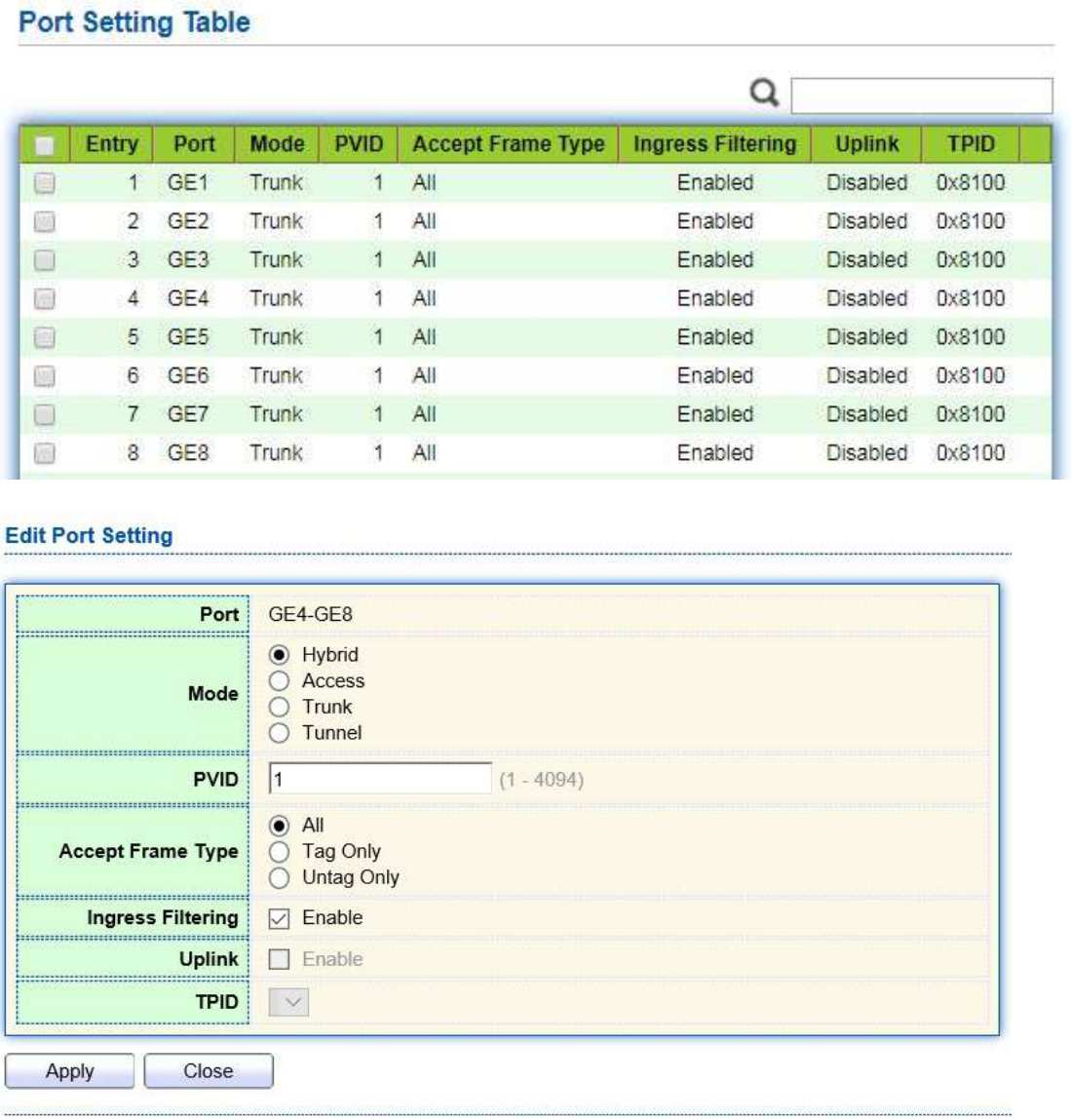
802.1q 프로토콜을 지원하는 각 스위치에서 보낸 패킷에는 스위치가 속한 VLAN 을 나타내는 VLAN ID 가 포함되어 있습니다. 따라서 VLAN 스위칭 네트워크에서 이더넷 프레임은 다음과 같이 두 가지 유형으로 구분됩니다.

- Tagged frame: 4 비트 802.1q 태그가 추가된 프레임을 말합니다.
- Untagged frame: 4 비트 802.1q 태그가 없는 원본 프레임을 나타냅니다.

다른 스위치와 연결되는 트렁크 인터페이스는 주로 트렁크 링크를 연결하여 VLAN 프레임이 흐르도록 합니다.

트렁크 인터페이스 구성 가이드:

1. 탐색 모음에서 " VLAN > VLAN > Port Setting "을 클릭하고 포트를 선택한 다음 "편집"하여 속성을 구성합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	구성할 포트 번호
Mode	포트의 VLAN 모드 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 멤버이자 VLAN 의 Tagged 멤버 역할을 합니다. Tunnel: 포트 Q-in-Q VLAN
PVID	포트 네이티브 VLAN

Accept Frame Type	포트에서 수신한 메시지 유형 All: 모든 메시지 Tag Only: 태그된 메시지만 수신됩니다 Untag Only: 태그가 지정되지 않은 메시지만 수신됩니다.
Ingress Filtering	포트에서 제외된 VLAN 메시지를 필터링하기로 결정하는 스위치
Uplink	업링크 모드인지 여부
TPID	VLAN 태그의 식별 번호

7.2 음성 VLAN

전통적으로 음성 데이터를 구별하기 위해 ACL(Access Control List)을 적용하고, 전송 품질을 보장하기 위해 QoS(Quality of Service)를 사용하여 우선순위를 높였습니다. 사용자 구성을 단순화하고 음성 흐름 관리를 용이하게 하기 위해 음성 VLAN 이 등장합니다. 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(조직 고유 식별자)를 확인하는 음성 데이터 흐름입니다. 음성 데이터 흐름을 수신하는 인터페이스는 자동으로 음성 VLAN 으로 전송되므로 사용자 구성 및 음성 데이터 관리가 단순화됩니다.

OUI of Voice VLAN

OUI 는 MAC 주소 필드를 나타냅니다. 해당 주소는 48 비트 MAC 주소와 해당 마스크 비트를 기반으로 계산할 수 있습니다. 수신 MAC 주소 및 일치하는 OUI 의 비트 수는 마스크의 모든 "1" 비트 길이에 따라 결정됩니다. 예를 들어 MAC 주소가 1-1-1 이고 마스크가 FFFF-FF00~0000 이라면 MAC 주소와 해당 마스크, 즉 OUI 를 실행하고 계산한 결과는 0001~0000~0000 이 됩니다.

수신 MAC 주소의 처음 24 비트가 OUI 의 주소와 일치하면 활성화된 음성 VLAN 인터페이스는 데이터 흐름과 수신 장치를 각각 음성 데이터 흐름과 음성 장치로 식별합니다.

Voice VLAN 은 사용자 Voice Data 흐름을 위해 구분됩니다. 음성 VLAN 은 음성 장치와 연결된 인터페이스를 연결하여 내부의 음성 데이터를 중앙 집중식으로 전송하기 위해 생성됩니다.

음성 데이터와 비음성 데이터가 동일한 네트워크에 존재하는 경우가 많습니다. 음성 데이터는 지연 가능성과 패킷 손실을 줄이기 위해 전송 중에 다른 비즈니스 데이터보다 더 높은 우선순위가 필요합니다.

1. 다음과 같이 탐색 표시줄에서 “VLAN > Voice VLAN > 프로퍼티”을 클릭합니다.

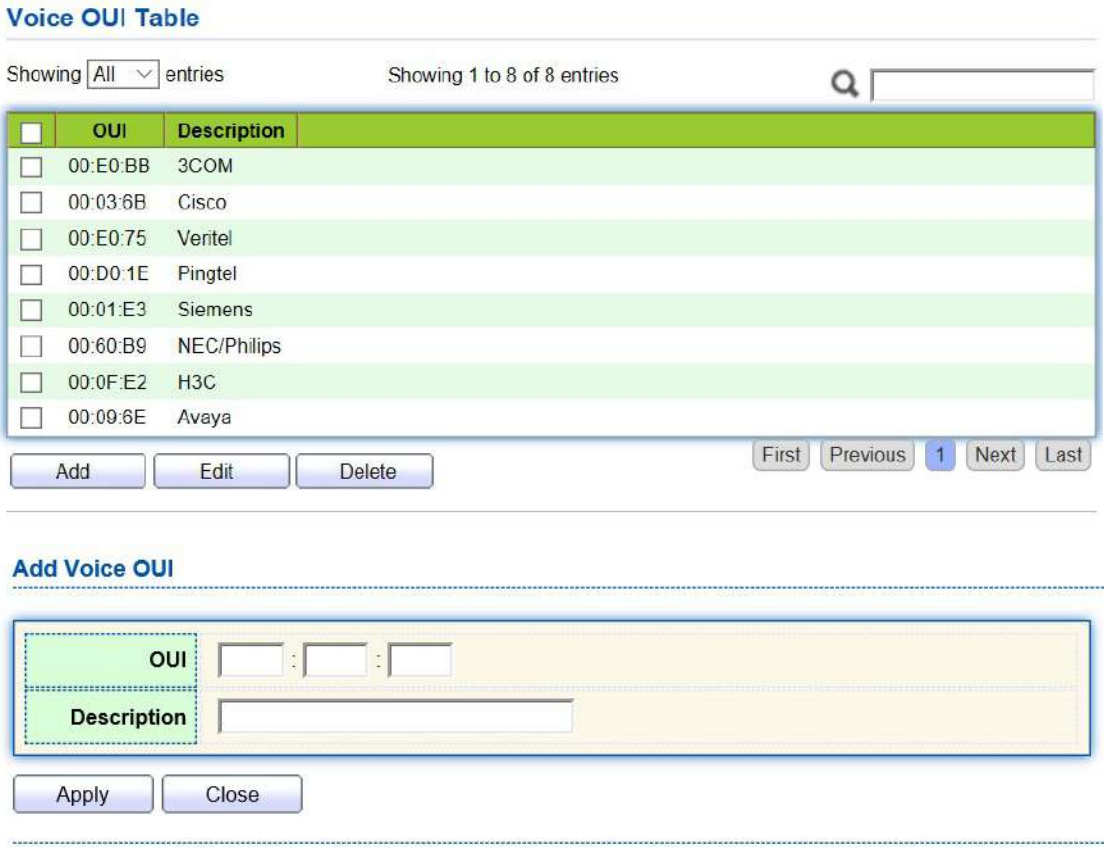
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
State	음성 VLAN 확인 및 활성화
VLAN	1~4,094 범위에서 추가된 VLAN ID 를 지정합니다. 1-3, 5, 7 및 9(기본적으로 VLAN 1 포함) 다른 VLAN 은 링크가 필요한 포트에 태그되지 않은 방식으로 추가되어야 합니다.
CoS / 802.1p Remarking	Voice VLAN 메시지 우선순위 재정의 여부
Aging Time	테이블 에이징 시간

인터페이스 데이터는 다음과 같습니다.

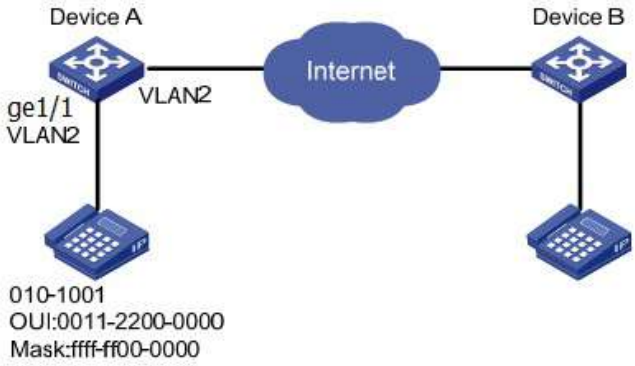
설정 항목	설명
Port	음성 VLAN 포트 활성화
State	음성 VLAN 확인 및 활성화
Mode	음성 VLAN 포트는 자동 모드와 수동 모드로 작동할 수 있습니다.
QoS Policy	QoS 의 영향을 받을 메시지를 선택하세요.

2. 탐색 표시줄에서 " VLAN > Voice VLAN > Voice OUI "를 클릭하여 다음과 같이 음성 VLAN 의 OUI 주소 세그먼트를 구성합니다.

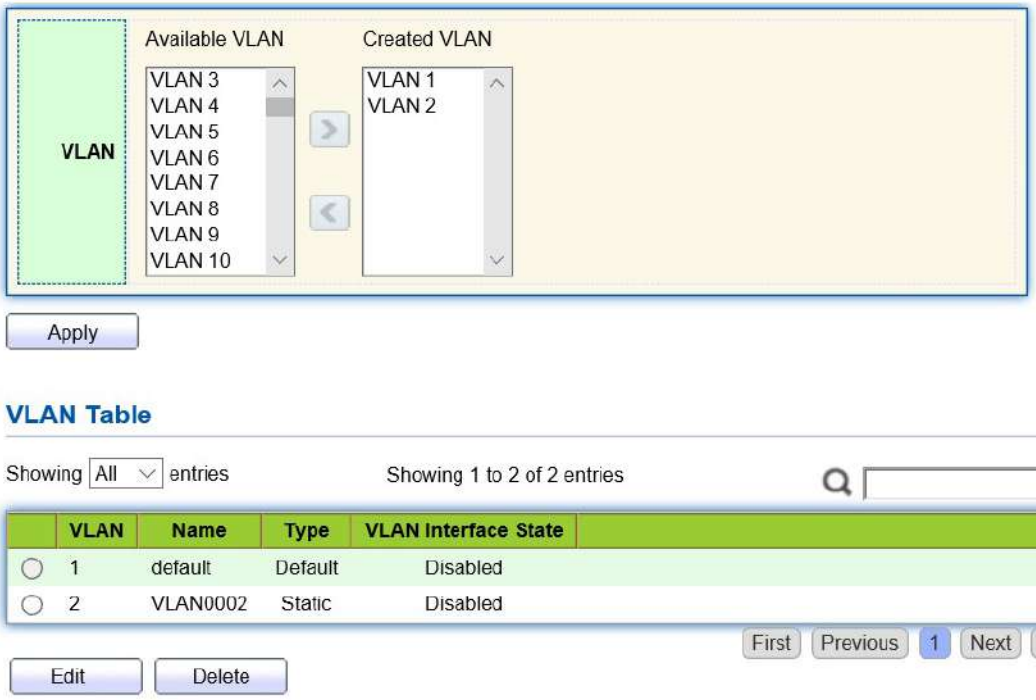


3. 해당 구성 항목을 입력합니다.
4. “적용”을 선택하고 다음과 같이 마무리합니다.

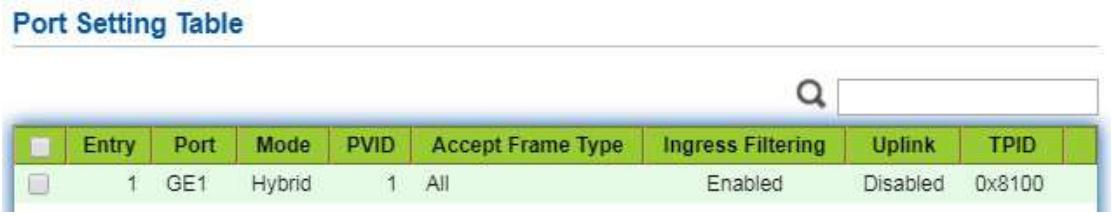
예를 들어, IP 텔레포니에 액세스하는 포트가 음성 VLAN 을 수신/송신하고 그 내에서 음성 흐름을 전송할 수 있도록 수동 모드에서 음성 VLAN 을 구성합니다. Voice VLAN 을 안전하게 운영하기 위해 VLAN2 를 생성하여 Voice Data 만 흐르게 합니다. IP 텔레포니는 태그 없는 음성 흐름을 수신 트렁크 포트인 GE1 으로 전송합니다. 사용자는 OUI(0011-2231-05e1)를 사용자 정의하고 자동 모드에서 음성 VLAN 네트워킹 다이어그램을 구성해야 합니다.



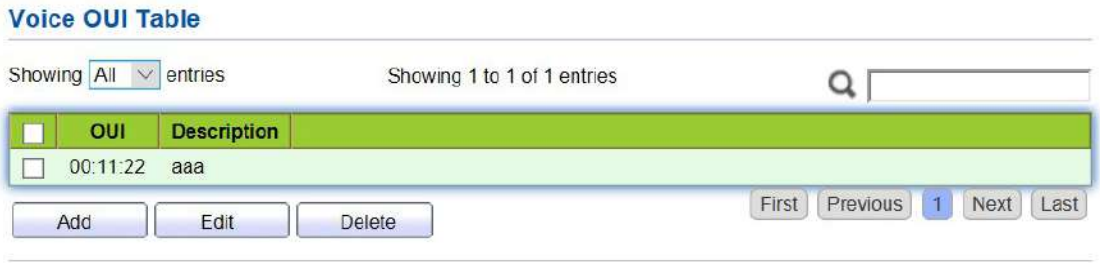
1. 직원이 속한 VLAN 을 인식하기 위해 VLAN 을 생성합니다. 탐색 표시줄에서 “VLAN > VLAN > Create VLAN”을 클릭하여 오른쪽 VLAN 목록에 VLAN 2 를 추가합니다. "적용"하고 완료합니다.



2. 하이브리드 모드에서 스위치 A 의 이더넷 인터페이스 GE1 을 구성합니다. 탐색 모음에서 " VLAN > VLAN > Port Setting "을 클릭하고 하이브리드 모드에서 GE1 을 "편집"합니다.



3. 탐색 표시줄에서 " VLAN > Voice VLAN > Voice OUI "를 클릭하여 OUI MAC 주소 범위를 구성 및 추가하고 음성 장치 MAC 주소의 처음 24 비트인 00:11:22 를 입력합니다. "적용"하고 다음과 같이 완료합니다.



4. 포트 GE1 의 음성 VLAN 을 활성화합니다. 탐색 표시줄에서 “VLAN > Voice VLAN > 프로퍼티”을 클릭하여 전역 구성을 활성화하고 VLAN2 를 선택합니다.

구성 목록 "편집"에서 포트 GE1 을 선택하고 자동 모드를 활성화합니다. "적용"하고 다음과 같이 완료합니다.

Note:

- 자동 모드가 활성화되면 VLAN2 에 포트가 없더라도 포트는 음성 VLAN 메시지를 전달합니다.

7.3 프로토콜 VLAN

프로토콜 VLAN 은 인터페이스에서 수신한 메시지의 프로토콜(패밀리) 유형 및 캡슐화 형식에 따라 다양한 VLAN ID 를 배포합니다.

관리자는 태그가 지정되지 않은 프레임이 수신되면 추가될 이더넷 프레임의 프로토콜 도메인과 VLAN ID 간의 매핑 체계를 준비해야 합니다. 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 변환해야 하므로 리소스 소모가 많아 속도가 느려집니다.

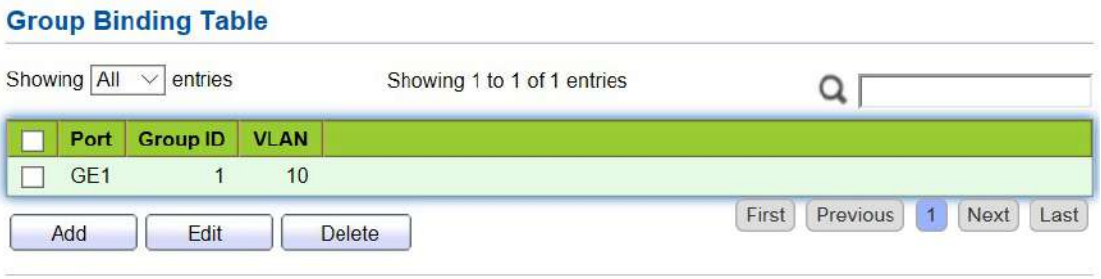
1. 다음과 같이 탐색 모음에서 " VLAN > Protocol VLAN > Protocol Group "을 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

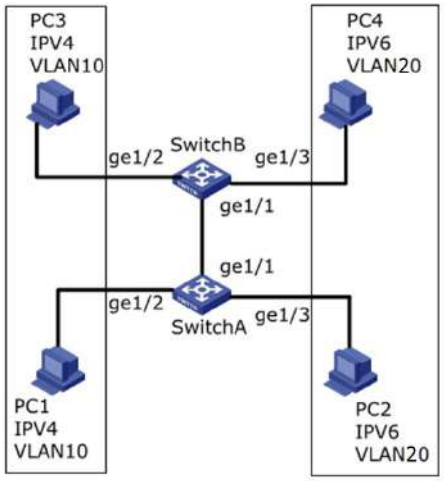
설정 항목	Description
Group ID	Protocol VLAN Group
Frame Type	Frame types: Ether2, LLC, RFC 1042
Protocol Value	It ranges from 0x600 to 0xFFFE

2. 해당 구성 항목을 입력합니다.
3. "적용"하고 마무리합니다.

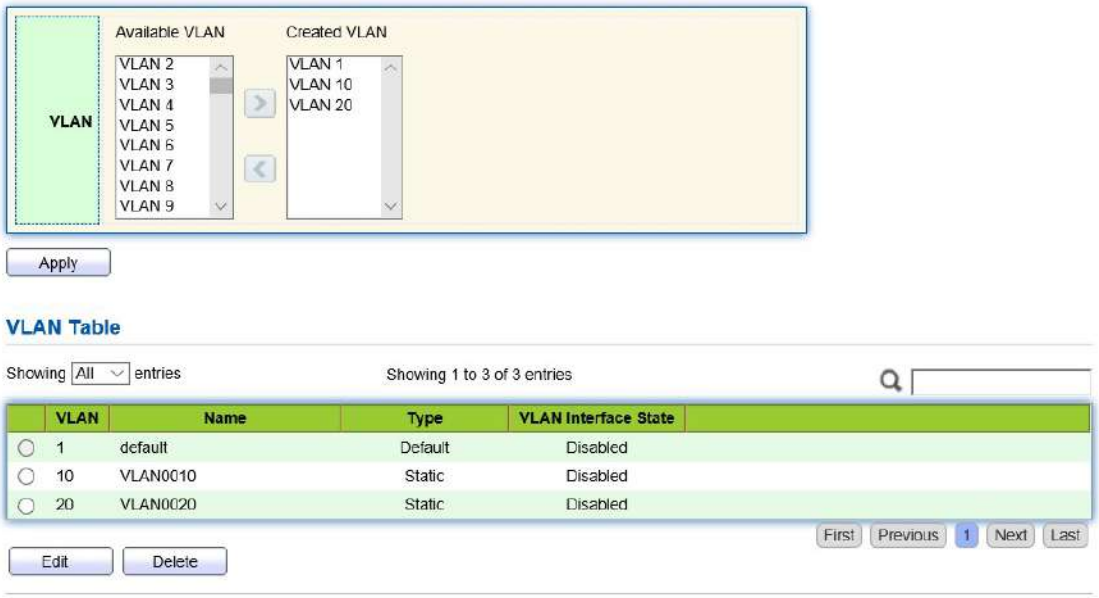
4. 탐색 모음에서 " VLAN > Protocol VLAN > Group Binding "을 클릭하여 프로토콜 번호, 포트 번호 및 VLAN ID 를 바인딩하고 다음과 같이 구성을 적용합니다.



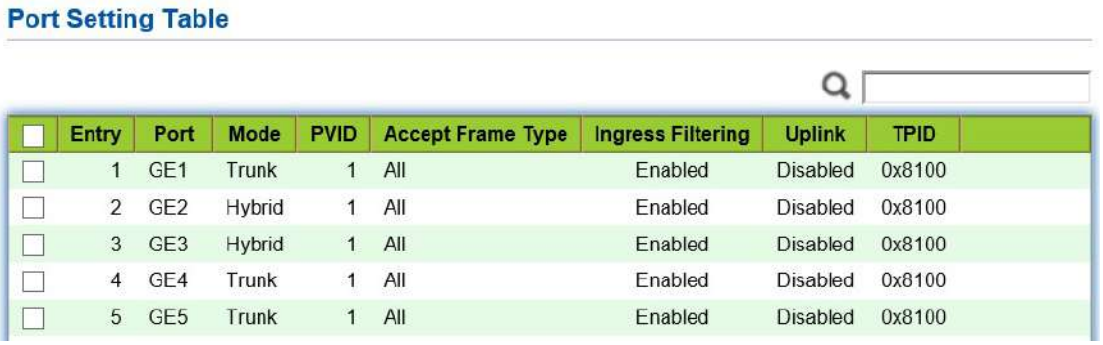
일치하는 프로토콜인 IPv4 및 IPv6 와 ARP 프로토콜을 구성합니다.
예를 들어 PC1 과 3 은 VLAN10 과 IPv4 통신 프로토콜 바인딩을 통해 상호 액세스할 수 있습니다. PC2 와 4 는 VLAN20 과 바인딩된 IPv6 통신 프로토콜을 통해 상호 액세스할 수 있습니다.
프로토콜 VLAN 분할의 네트워킹 다이어그램



1. 직원이 속한 VLAN 을 인식하기 위해 VLAN 을 생성합니다. " VLAN > VLAN > Create VLAN "을 클릭하고 오른쪽의 VLAN 생성 목록에 VLAN10 과 20 을 추가한 후 "Apply"를 클릭하고 완료합니다.



2. 하이브리드 모드에서 스위치 A 의 GE2 및 GE3 인터페이스를 구성합니다. " VLAN > VLAN > Port Setting "을 클릭하고 하이브리드 모드에서 인터페이스를 "편집"합니다.



3. Untagged GE2 와 GE3 을 VLAN10 과 VLAN20 에 각각 추가합니다. " VLAN > VLAN > VLAN Configuration "을 클릭하고 목록을 드롭다운하여 VLAN10 및 Untagged GE2 포트를 선택합니다. 동일한 단계에 따라 다음과 같이 태그가 지정되지 않은 GE3 를 VLAN20 에 추가합니다.

4. 링크가 필요한 포트가 있는 VLAN 에 스위치 B 의 태그 없는 GE2 및 GE3 인터페이스를 추가합니다. 단계는 2 단계와 3 단계와 같습니다.
5. 스위치 A 의 Tagged GE1 인터페이스를 VLAN10 및 20 에 추가합니다. " VLAN > VLAN > VLAN Configuration "을 클릭하고 목록을 드롭다운하여 VLAN10 과 GE1 의 Tagged 멤버를 선택합니다. VLAN20 도 비슷하게 구성합니다.

6. 관련 프로토콜 및 VLAN. VLAN ID 는 인터페이스에서 수신한 메시지의 프로토콜(패밀리) 유형 및 캡슐화 형식에 따라 할당됩니다. 탐색 모음에서 " VLAN > Protocol VLAN > Protocol Group "을 클릭하여 프로토콜 그룹에 대한 2 개의 규칙을 추가합니다.

7. 포트, 프로토콜 그룹 및 VLAN 바인딩. “VLAN > Protocol Group > Group

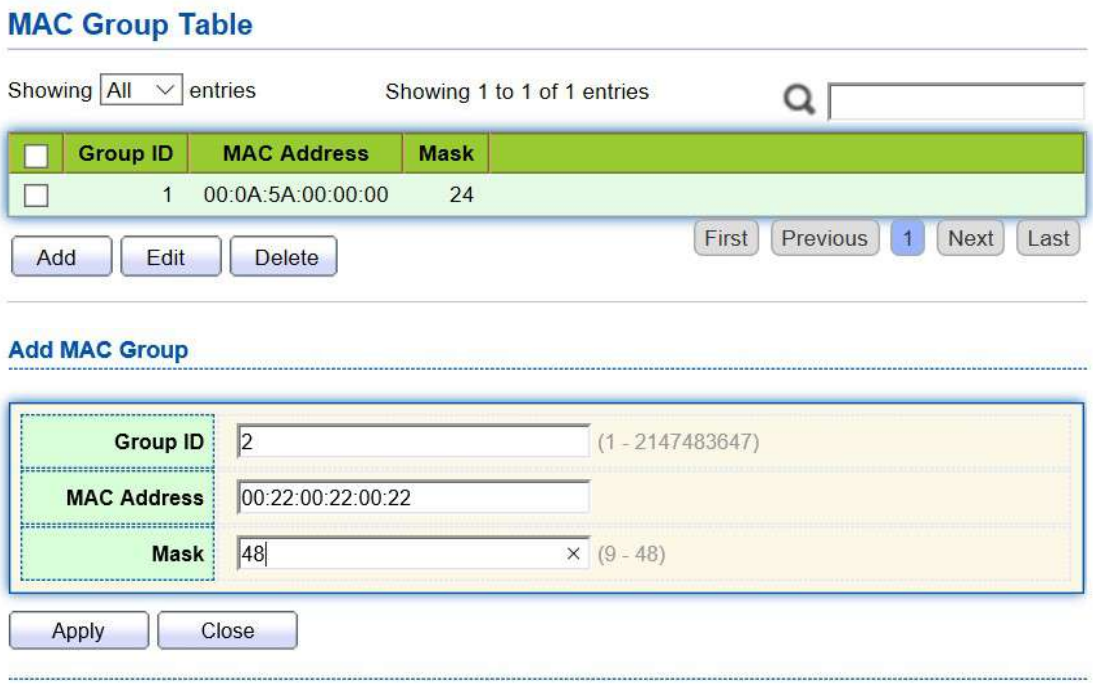
Binding", "추가"를 클릭하여 GE2 와 그룹 ID1 을 VLAN10 에 바인딩하고, GE3 및 그룹 ID2 를 VLAN20 에 바인딩합니다.

7.4 MAC VLAN

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

장점: 터미널 사용자의 물리적 위치가 변경될 때 VLAN 을 재구성할 필요가 없으므로 사용자 보안과 액세스 유연성이 보장됩니다. 단점: 사전에 멤버를 정의하여 네트워크 카드 및 단순 네트워크 환경을 자주 교체하지 않는 현장에 적용됩니다.

1. 탐색 모음에서 " VLAN > MAC VLAN > MAC Group "을 클릭하고 다음과 같이 새 MAC 그룹을 "추가"합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Group ID	MAC VLAN 그룹 ID
MAC Address	VLAN 과 바인딩할 MAC 주소
Mask	MAC 주소 포트를 나타냅니다. 정확히 일치하는 경우 48 을 입력하세요. 다른 것들은 IP 주소 마스크와 일치해야 합니다.

예를 들어, 정보 보안 요구 사항이 높은 회사에서는 PC 가 내부 네트워크에만 액세스하도록 허용합니다. 그림과 같이 스위치 GE1 은 스위치 A 의 업링크 포트를 연결하고 다운스트림 포트는 PC1, 2, 3 을 연결합니다. 결과적으로 PC1, 2, 3 은 스위치 A 와 스위치를 통해 내부 네트워크에 액세스할 수 있지만 다른 PC 는 액세스할 수 없습니다. .

구성 논리: MAC 주소를 기준으로 VLAN 을 나누는 데 다음 단계가 사용됩니다.

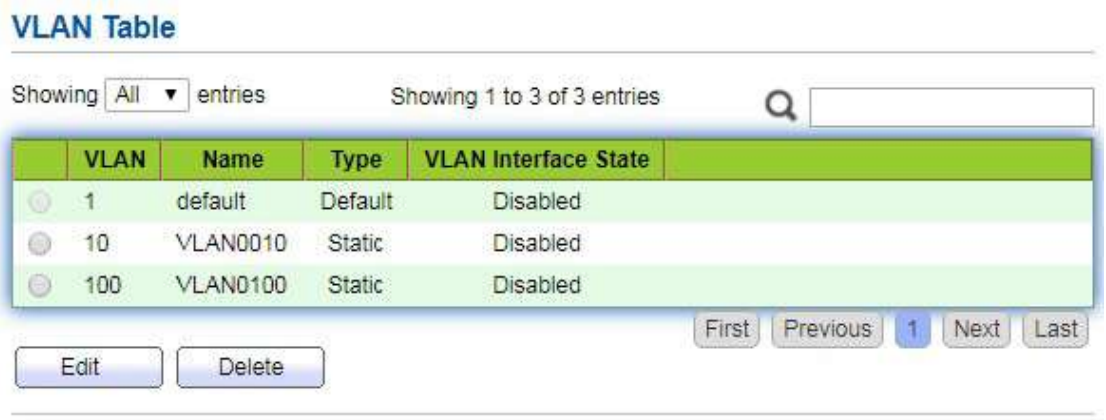
1. 관련 VLAN 을 생성합니다.
2. 올바른 방법으로 VLAN 에 이더넷 인터페이스를 추가합니다.
3. PC1, 2, 3 의 MAC 주소에 VLAN 을 연결합니다.

데이터 준비: 구성 인스턴스에 대해 다음 데이터를 준비해야 합니다.

- 스위치에서 GE1 PVID 를 100 으로 설정합니다.
- 스위치에서 Untagged 방식으로 VLAN10 에 액세스하도록 GE1 을 설정합니다.
- 스위치의 태그 방식으로 VLAN10 에 액세스하도록 GE2 를 설정합니다.
- 스위치 A 인터페이스를 기본적으로 설정합니다. 즉, 모든 인터페이스가 태그되지 않은 방식으로 VLAN1 에 추가됩니다.
- PC1, 2, 3 의 MAC 주소를 VLAN10 에 연결합니다.

MAC 주소를 기반으로 VLAN 분할에 대한 네트워킹 다이어그램을 그립니다.

1. 직원이 속한 VLAN 을 인식하기 위해 VLAN 을 생성합니다. 네비게이션 바에서 “VLAN > VLAN > Create VLAN”을 클릭하고 오른쪽 VLAN 생성 목록에 VLAN10 을 추가한 후 “적용”하고 다음과 같이 완료합니다.



2. VLAN10 의 태그되지 않은 구성원 역할을 하도록 PVID 가 100 인 하이브리드 모드에서 스위치의 GE1 을 구성합니다. VLAN10 의 태그된 멤버 역할을 하도록

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 인터페이스는 태그가 지정되지 않은 방식으로 VLAN1 에 액세스합니다. PC1, 2, 3 의 MAC 주소를 VLAN10 에 연결합니다. 탐색 표시줄에서 " VLAN > MAC VLAN > MAC Group "을 클릭하고 PC1(0022-0022-0022), PC2(0033-0033-0033) 및 PC3(0044-0044-0044)의 MAC 주소를 입력합니다. 48 비트 완전 일치 마스크는 다음과 같습니다.

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

Add Edit Delete First Previous 1 Next Last

4. 탐색 모음에서 " VLAN > MAC VLAN > Group Binding "을 클릭하고 "추가"를 클릭하여 하이브리드 포트만 선택하고 바인딩할 MAC 그룹 ID 와 지정된 VLAN ID 를 선택합니다. "적용"하고 완료합니다.

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

Add Edit Delete First Previous 1 Next Last

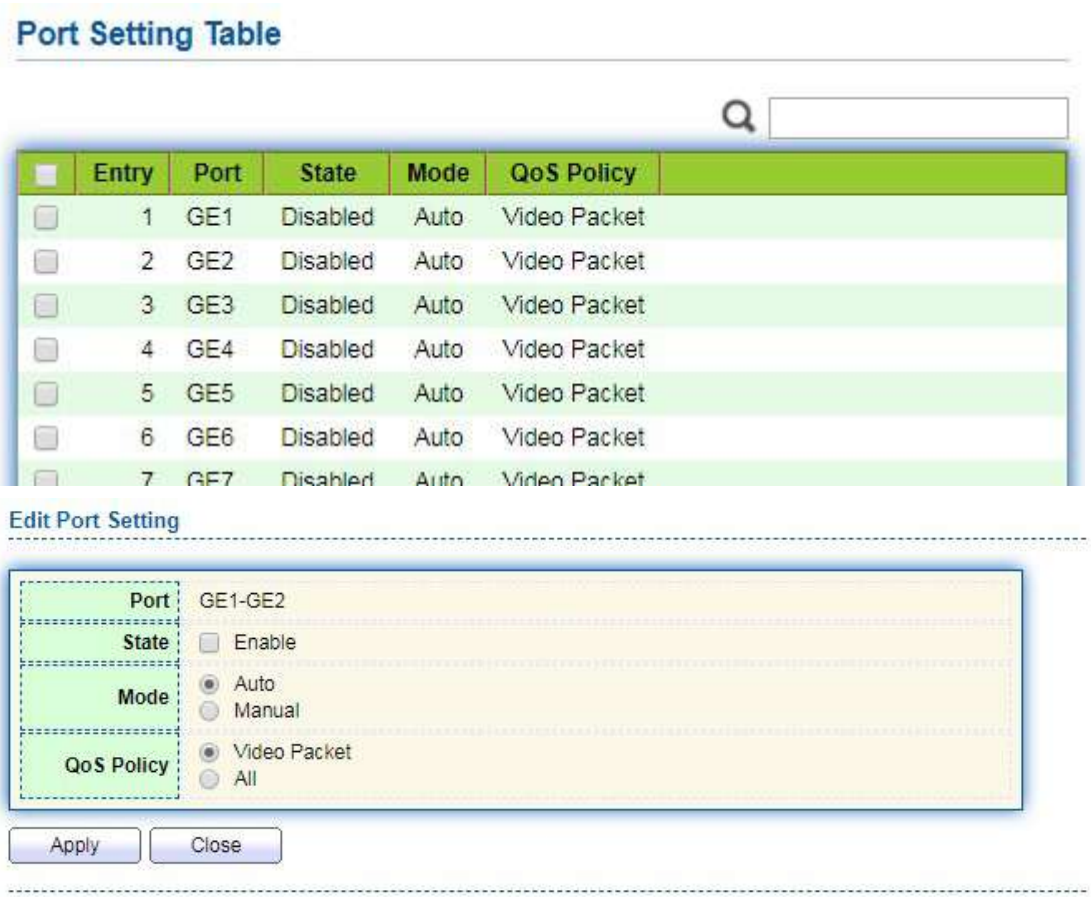
5. 구성 확인
PC1, 2, 3 만 내부 네트워크에 접근할 수 있습니다..

7.5 감시 VLAN

감시 VLAN 은 주로 비디오 스트림 패킷에 사용됩니다. 전송 과정에서 이러한 패킷의 우선 순위를 보장하기 위해 일반 패킷보다 높습니다.

1. 다음과 같이 탐색 표시줄에서 “VLAN > Surveillance VLAN > 프로퍼티”을 클릭합니다.

설정 항목	설명
State	감시 VLAN 확인 및 활성화
VLAN	1~4,094 범위에서 추가된 VLAN ID 를 지정합니다. 1-3, 5, 7 및 9(기본적으로 VLAN 1 포함) 다른 VLAN 은 링크가 필요한 포트에 태그되지 않은 방식으로 추가되어야 합니다.
CoS / 802.1p Remarking	Voice VLAN 메시지 우선순위 재정의 여부
Aging Time	테이블 에이징 시간



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	음성 VLAN 포트 활성화
State	감시 VLAN 확인 및 활성화
Mode	감시 VLAN 포트는 자동 모드와 수동 모드로 작동할 수 있습니다.
QoS Policy	QoS 의 영향을 받을 메시지를 선택하세요.

2. 탐색 모음에서 " VLAN > Surveillance VLAN > Surveillance OUI "를 클릭하여 감시 VLAN 의 OUI 주소 세그먼트를 다음과 같이 구성합니다.

3. 해당 구성 항목을 입력합니다.
4. “적용”을 선택하고 다음과 같이 마무리합니다.

7.6 GVRP

GVRP VLAN 등록 프로토콜은 802.1Q 호환 VLAN 제거 기능과 802.1Q 트렁크 포트 트렁크 포트에 대한 동적 VLAN 설정을 제공하는 일반 속성 등록 프로토콜의 응용 프로그램입니다.

GVRP 스위치는 서로 VLAN 구성 정보를 교환하고, 불필요한 브로드캐스트 및 알 수 없는 유니캐스트 트래픽을 차단하며, 802.1Q 트렁크를 통해 연결된 스위치에서 VLAN 을 동적으로 생성 및 관리할 수 있습니다.

GID 와 GIP 는 각각 GARP 기반 애플리케이션에 대한 일반적인 상태 메커니즘 설명과 정보 배포 메커니즘을 제공하는 GVRP 에서 사용됩니다. GVRP 는 802.1Q 트렁크 링크에서만 실행됩니다. GVRP 는 트렁크 연결을 통해 활성 VLAN 만 전송되도록 트렁크 링크를 차단합니다. GVRP 는 VLAN 을 트렁크 라인에 추가하기 전에 먼저 스위치로부터 가입 정보를 받습니다. GVRP 업데이트 정보 및 타이머를 변경할 수 있습니다. GVRP 포트에는 VLAN 을 조정하는 방법을 제어할 수 있는 다양한 작동 모드가 있습니다. GVRP 는 VLAN 데이터베이스에 대한 VLAN 을 동적으로 추가하고 관리할 수 있습니다.

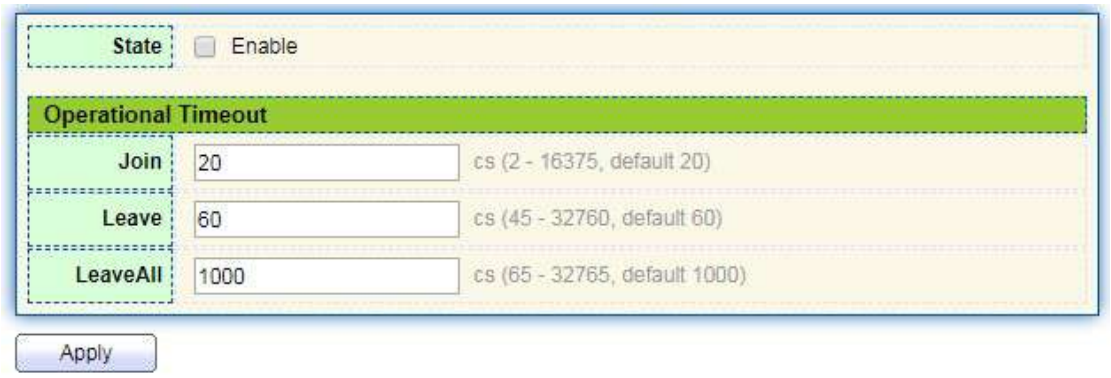
GVRP 는 장치 간 VLAN 정보 전파를 지원합니다. GVRP 에서는 스위치의 VLAN 정보를 수동으로 구성할 수 있으며 네트워크의 다른 모든 스위치는 VLAN 을 동적으로 이해할 수 있습니다. 터미널 노드는 모든 스위치에 액세스하고 필요한 VLAN 에 연결할 수 있습니다. GVRP 를 사용하려면 GVRP 호환 네트워크 인터페이스 카드(NIC)를 설치해야 합니다. GVRP 호환 NIC 는 필요한 VLAN 에

가입한 다음 GVRP 지원 스위치에 액세스하도록 구성할 수 있습니다. NIC 와 스위치 사이의 통신 연결이 설정되고, NIC 와 스위치 사이에 VLAN 연결이 실현됩니다.

7.6.1 프로퍼티

전역 및 포트 구성

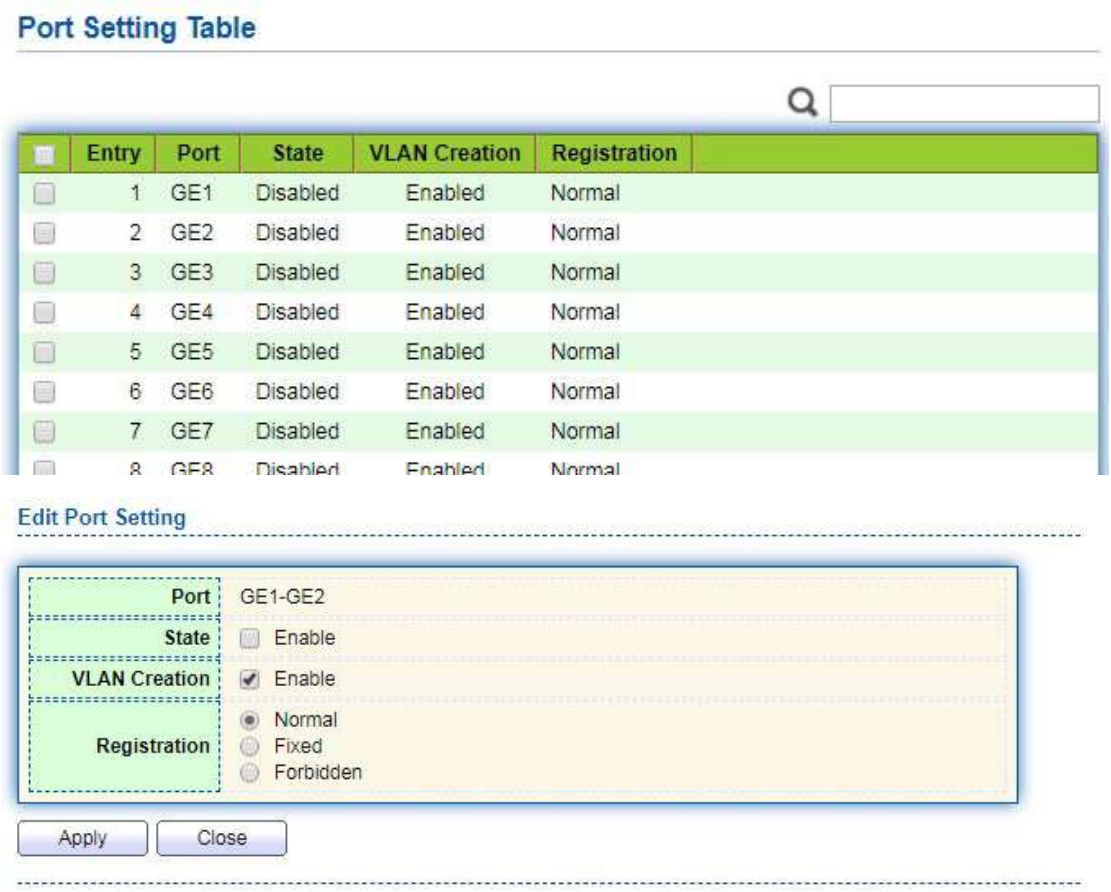
1. 다음과 같이 탐색 표시줄에서 “VLAN > GVRP > 프로퍼티”을 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
State	GVRP 기능은 다음 설정을 통해 전역적으로 활성화됩니다.
Join	2~16375cs 범위의 값(즉, 100 분의 1 초 단위)입니다. 기본값은 20cs 입니다.
leave	45~32760cs 범위의 값, 즉 1/100 초 단위입니다. 기본값은 60cs 입니다.
LeaveAll	65~32765cs 범위의 값, 즉 1/100 초 단위입니다. 기본값은 1000cs 입니다.

2. 탐색 표시줄에서 " VLAN > GVRP > 프로퍼티 "을 클릭하고 포트를 선택한 다음 "편집"을 선택하여 다음과 같이 구성 인터페이스로 들어갑니다.



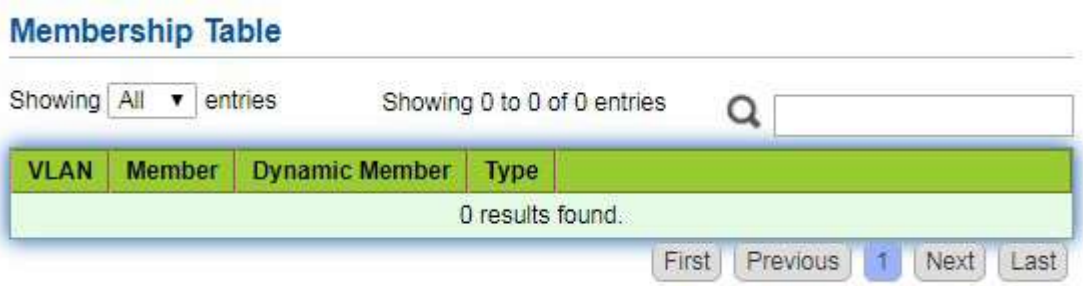
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
State	포트의 GVRP 기능을 활성화 또는 비활성화합니다.
VLAN Creation	VLAN 자동 생성 활성화 또는 비활성화
Registration	GVRP 의 세 가지 등록 모드 일반: 동적 VLAN 이 포트에 등록되도록 허용하고 정적 VLAN 과 동적 VLAN 의 선언 메시지를 동시에 보냅니다. 수정됨: 동적 VLAN 은 포트에 등록할 수 없으며 정적 VLAN 선언 메시지만 전송됩니다. 금지됨: 동적 VLAN 은 포트에 등록할 수 없습니다. 동시에 해당 포트의 vlan1 을 제외한 모든 VLAN 이 삭제되고 vlan1 선언 메시지만 전송됩니다.

7.6.2 맴버십

GVRP 동적 회원 정보 보기

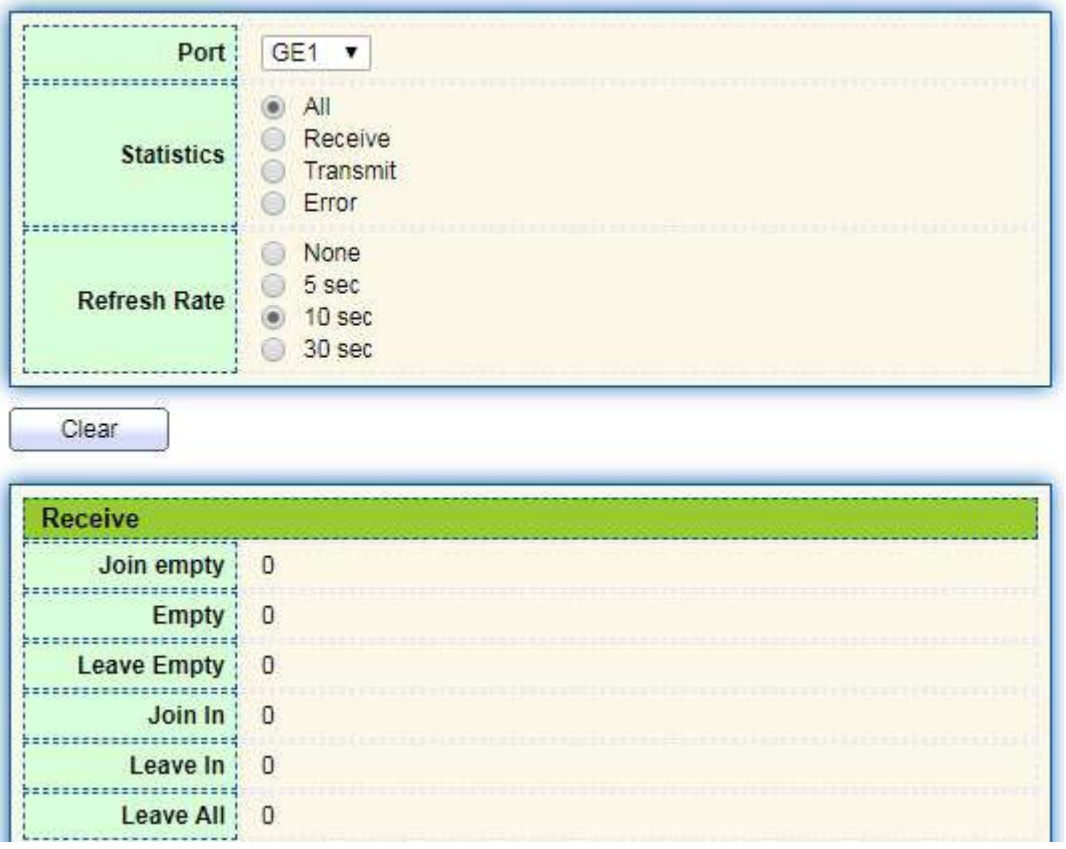
1. 다음과 같이 탐색 표시줄에서 “VLAN > GVRP > Membership”을 클릭합니다.



7.6.3 통계

포트 GVRP 메시지 통계 보기

1. 다음과 같이 탐색 표시줄에서 “VLAN > GVRP > Statistics”를 클릭합니다.



8 맥 주소 테이블

이더넷 스위치는 주로 데이터 링크 계층에서 목적에 따라 전달하도록 혁신되었습니다. 즉, MAC 주소는 목적에 따라 해당 포트로 메시지를 전송하게 됩니다. MAC 주소 전달 테이블은 L2 메시지의 빠른 전달의 기본이 되는 MAC 주소와 전달 포트를 나타내는 L2 테이블입니다.
MAC 주소 전달 테이블에는 다음 데이터가 포함됩니다.

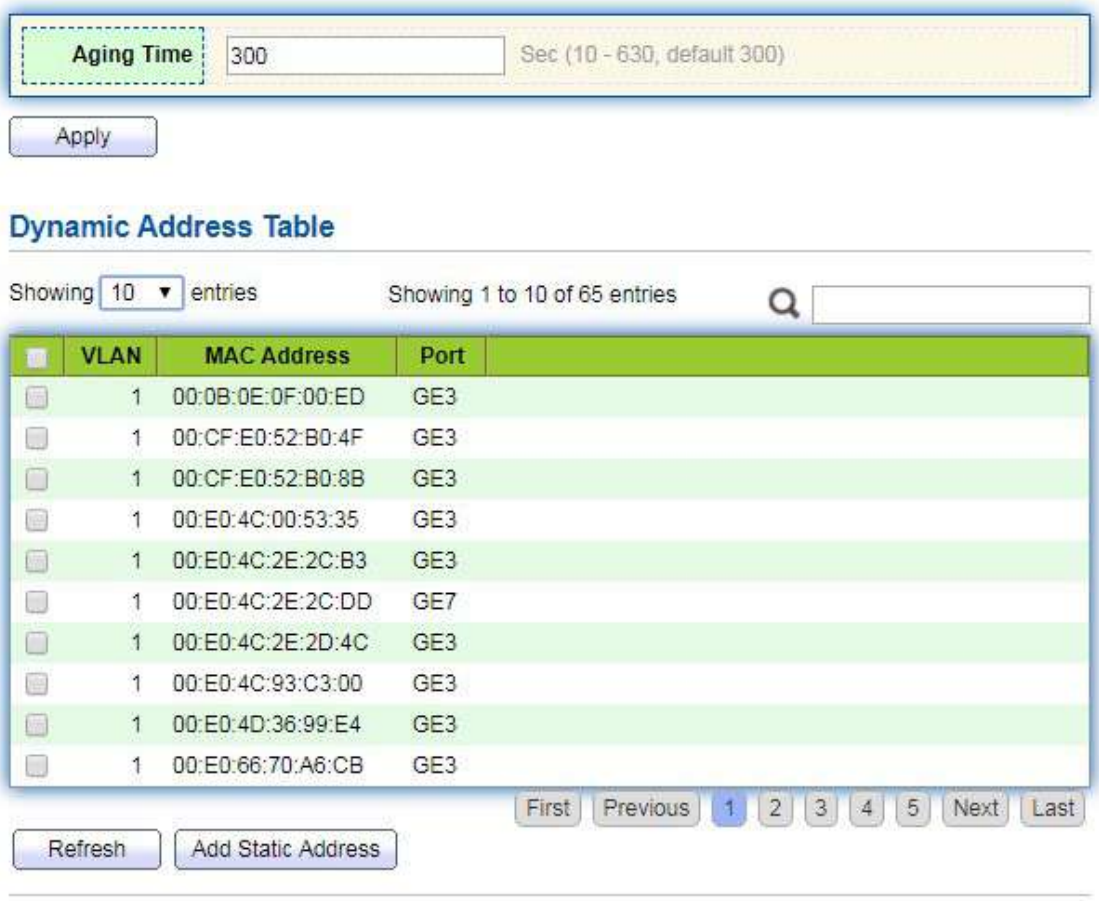
- 목적지 MAC 주소
- 포트에 속한 VLAN ID
- 이 장치의 전달 수신 번호

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

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

8.1 동적 주소

이 페이지에서는 MAC 주소의 에이징 시간과 테이블 정보를 구성하고 확인할 수 있습니다.
MAC 주소 테이블은 네트워크 변경 사항에 맞춰 지속적인 업데이트가 필요합니다. 수명(예: 에이징 시간)에 따라 제한되는 항목을 자동으로 생성합니다. 만료 후 새로 고쳐지지 않은 항목은 삭제됩니다. 만료되기 전에 해당 레코드를 새로 고치면 항목의 에이징 시간이 다시 계산됩니다.
적절한 에이징 시간은 MAC 주소의 에이징 목표를 달성하는 데 도움이 됩니다. 에이징 시간이 부족하면 많은 스위치가 대상 MAC 주소의 패킷을 검색하기 위해 브로드캐스트되어 스위치 성능에 영향을 미칠 수 있습니다.
너무 오래 에이징하면 스위치가 오래된 MAC 주소 항목을 저장하게 되어 전달 리소스가 소진되고 네트워크 변경 사항에 따라 전달 테이블을 업데이트하지 못할 수 있습니다.
스위치는 에이징 시간이 너무 짧기 때문에 유효한 MAC 주소 테이블 항목을 제거하여 전달 효율성을 감소시킬 수 있습니다. 일반적으로 권장되는 에이징 시간은 기본적으로 300 초입니다.
노화 시간 설정 가이드:
1. 구성 및 보기 인터페이스에 대한 탐색 모음에서 " MAC Address Table > Dynamic Address "를 클릭합니다.



인터페이스 데이터는 다음과 같습니다

설정 항목	설명
MAC Aging Time	MAC 주소의 에이징 시간을 입력하세요.

2. 해당 구성 항목을 입력합니다.
3. “적용"하고 마무리합니다.

MAC 테이블은 스위치가 학습한 MAC 주소, VLAN 번호, Ingress/Egress 정보 등을 저장합니다. 데이터를 전달할 때 대상 MAC 주소와 이더넷 프레임의 VLAN 번호 쿼리 테이블에 따라 장치 출구를 빠르게 찾습니다.

MAC 주소 테이블을 확인하려면 3 장의 3.3 절을 참조하세요.

8.2 정적 주소

정적 테이블은 사용자가 수동으로 구성하고 각 인터페이스 보드에 배포되므로 오래되지 않습니다.

1. 다음과 같이 “MAC Address Table > Static Address”를 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

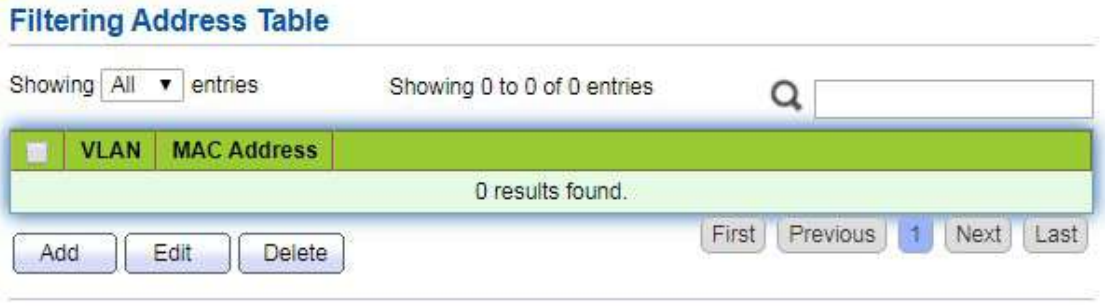
설정 항목	설명
MAC	필수. 새 MAC 주소를 입력하세요(예: HH:HH:HH:HH:HH:HH)
VLAN	필수. VLAN ID 지정
Port	필수. 인터페이스 유형을 선택하고 인터페이스 이름을 입력하세요.

2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

8.3 주소 필터링

스위치는 구성에 따라 일치하는 데이터 프레임을 삭제합니다.

1. 다음과 같이 "MAC Address Table > Filtering Address"을 클릭하세요.



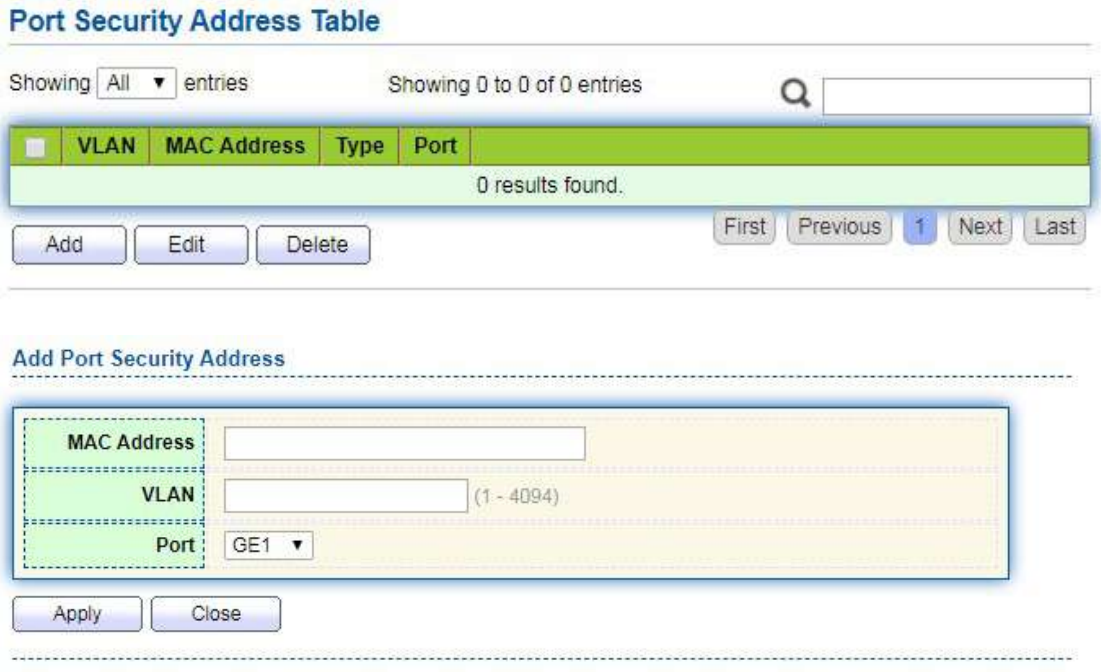
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
MAC Address	필터링할 MAC 주소
VLAN	MAC 주소의 VLAN

8.4 포트 보안 주소

MAC 주소가 보안 Mac 으로 설정된 경우 포트는 보안 Mac 의 데이터 프레임만 영원히 통과하도록 허용하고 나머지는 삭제됩니다.

1. 다음과 같이 “MAC Address Table > Port Security Address”를 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
MAC Address	보안을 위한 MAC 주소

VLAN	MAC 주소의 VLAN
Port	포트 보안을 활성화하는 포트 ID

9 스패닝 트리

이더넷 스위칭 네트워크에서는 링크 백업과 네트워크 안정성을 위해 중복 링크가 자주 사용됩니다. 그러나 이러한 링크는 스위칭 네트워크에 루프를 생성하여 브로드캐스트 폭풍, 불안정한 MAC 주소 목록 및 기타 오류를 발생시켜 사용자의 통신 품질을 저하시키거나 심지어 통신을 중단시킬 수도 있습니다. 결과적으로 STP(Spanning Tree Protocol)가 나타납니다.

IEEE 802.1D 에 정의된 원본 STP 부터 IEEE 802.1W 에 정의된 RSTP(Rapid Spanning Tree Protocol), IEEE 802.1S 에 정의된 MSTP(Multiple Spanning Tree Protocol)에 이르기까지 다른 프로토콜의 개발과 마찬가지로 STP 도 계속 업그레이드되고 있습니다.

MSTP 는 RSTP 및 STP 와 호환되고 RSTP 는 STP 와 호환됩니다. 이 3 가지 프로토콜 간의 대조가 표에 나와 있습니다.

3 가지 프로토콜의 대조

STP	특성	응용
STP	폭주 및 중복 백업을 방송하기 위한 솔루션으로 루프를 제거한 트리입니다. 천천히 수렴됩니다.	모든 VLAN 은 사용자 또는 비즈니스 흐름에 차별 없이 공유될 수 있습니다.
RSTP	폭주 및 중복 백업을 방송하기 위한 솔루션으로 루프를 제거한 트리입니다. 빠르게 수렴됩니다.	
MSTP	폭주 및 중복 백업을 방송하기 위한 솔루션으로 루프를 제거한 트리입니다. 빠르게 수렴됩니다. 스패닝 트리는 VLAN 간에 로드 균형을 조정합니다. 다양한 VLAN 의 흐름은 경로에 따라 전달됩니다.	로드 공유를 위한 사용자 흐름과 비즈니스 흐름을 구별합니다. 서로 다른 VLAN 은 별도의 스패닝 트리를 통해 흐름을 전달합니다.

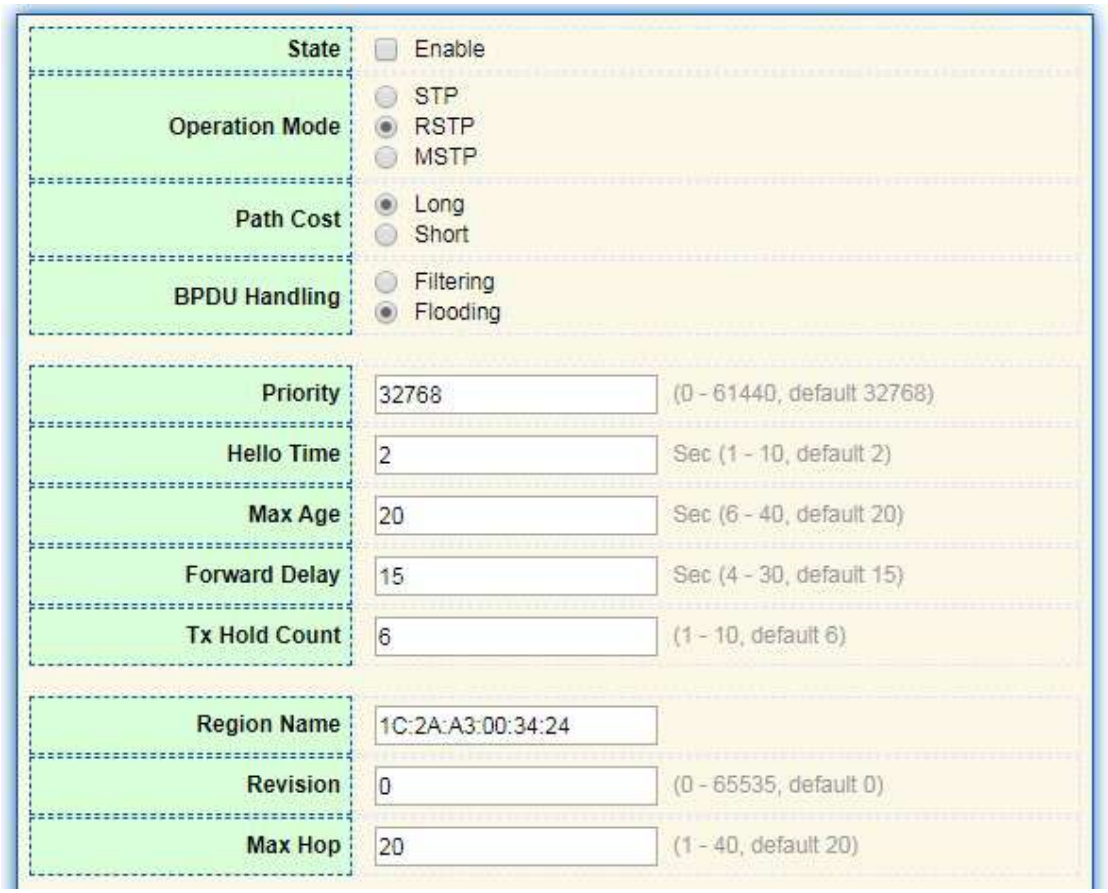
STP 가 배포된 후 토폴로지를 사용하여 루프를 계산하면 다음 목표를 달성할 수 있습니다.

- Loop elimination: 중복 링크를 차단하여 가능한 통신 루프를 제거합니다..
- Link backups: 활성 경로가 실패하는 경우 중복 링크를 활성화하여 네트워크 연결을 복원하세요..

9.1 프로퍼티

STP 전역 매개변수를 구성합니다. 특정 네트워크 환경에서는 최상의 성능을 얻으려면 일부 장치의 STP 매개변수를 조정해야 합니다.

1. 다음과 같이 탐색 표시줄에서 “Spanning Tree > 프로퍼티”을 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
State	스위치 대신 스패닝 트리를 활성화하려면 기본적으로 선택되어 있습니다.
Operation Mode	STP, RSTP, MSTP 의 3 가지 모드를 사용할 수 있습니다.
Path Cost	롱 모드와 쇼트 모드에서
BPDU Handling	장치가 수신한 BPDU 메시지를 처리하는 방법
Priority	포트 우선순위
Hello Time	Hello 메시지 사이의 간격
Max Age	최대 노화 시간
Forward Delay	순방향 지연 시간

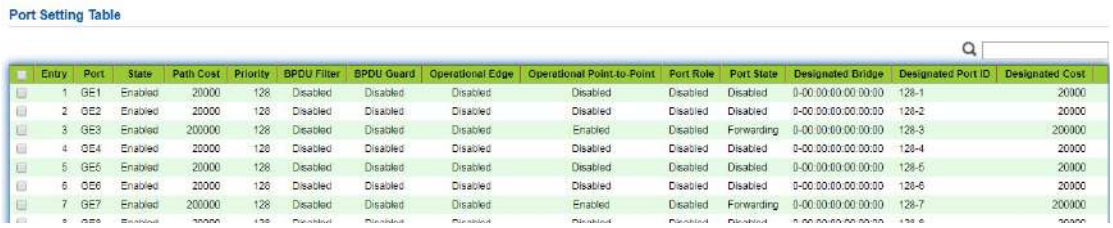
Tx Hold Count	초당 최대 패킷 전송 수를 제한하는 데 사용되는 Tx-hold-count 를 지정합니다.
Region Name	MST 도메인 이름. 스위치 마스터 보드는 기본적으로 MAC 주소를 설정합니다. MST 도메인의 VLAN 매핑 테이블 및 MSTP 의 개정 수준과 함께 스위치 도메인 이름은 자신이 속한 도메인을 공동으로 결정합니다.
Revision	MSTP 개정 번호
Max Hop	BPDU 가 삭제되기 전 MSTP 영역의 홉 수를 지정합니다.

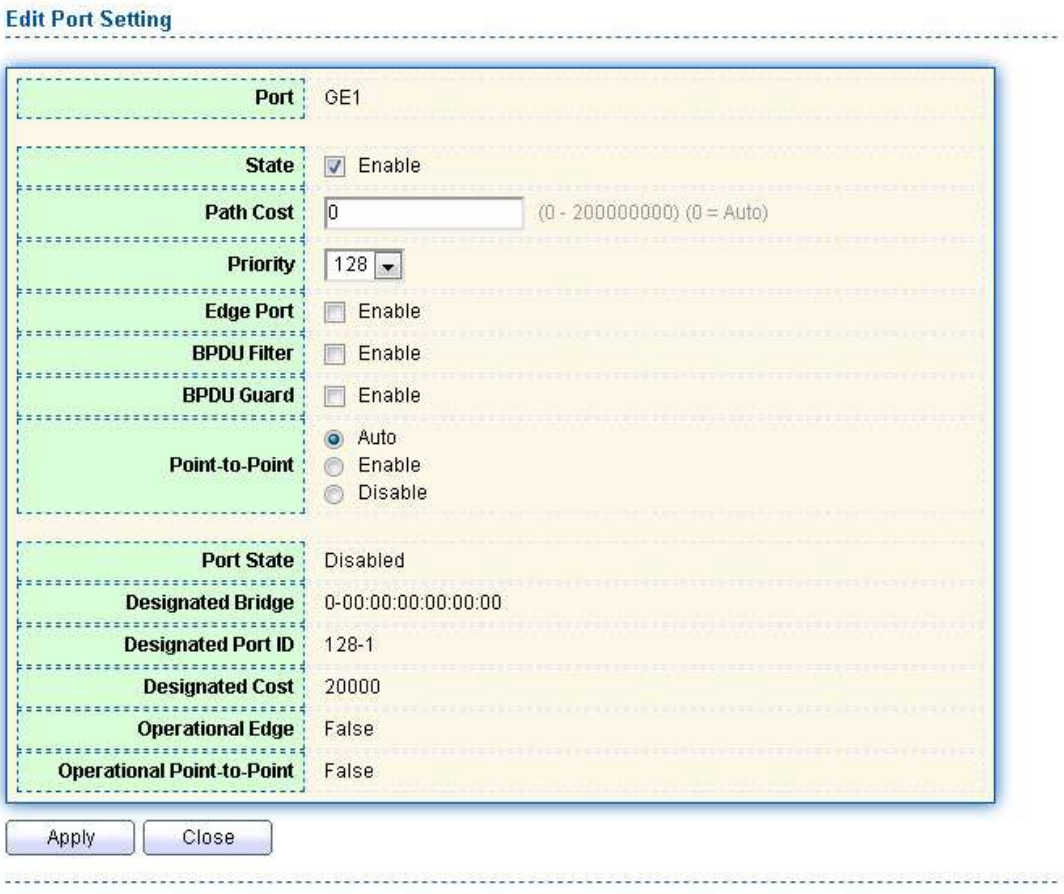
2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

9.2 포트 설정

특정 네트워크 환경에서는 최상의 성능을 위해 일부 장치의 STP 매개변수를 조정해야 합니다.

1. 탐색 모음에서 " Spanning Tree > Port Setting "을 클릭하고 포트를 선택한 다음 "편집"을 선택하여 해당 속성을 구성합니다.





인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	속성을 구성하는 포트 번호
State	STP 활성화 여부
Path Cost	인터페이스의 경로 비용 값을 입력합니다. 0~200,000,000 범위의 값으로 IEEE 802.1t 표준을 사용합니다.
Priority	더 높은 우선순위를 나타내는 작은 값으로 포트 우선순위를 선택하십시오. 인터페이스 우선순위는 지정된 MSTI 의 인터페이스 역할에 영향을 미칩니다. 다른 MSTI 에서 사용자는 동일한 인터페이스에 대한 우선순위를 구성할 수 있습니다. 결과적으로 다양한 VLAN 의 흐름이 물리적 링크를 따라 전달되어 VLAN 로드 공유를 달성할 수 있습니다. 설명: MSTP 는 인터페이스 역할을 다시 계산하고 우선 순위가 변경되면 해당 상태를 마이그레이션합니다.
Edge Port	다른 스위치나 네트워크 세그먼트가 아닌 에지 포트를 사용자 단말기에 직접 연결해야 합니다. 토폴로지 변경으로 인해 루프가 생성되지 않으므로 신속하게 전달 상태로 전환할 수 있습니다. 구성 중인 에지 포트는 STP 를 통해 신속하게 전달 상태로 전환될

	수 있습니다. 이를 위해서는 사용자 단말에 직접 연결된 이더넷 포트를 에지 포트로 구성하는 것이 좋습니다.
BPDU Filter	BPDU 필터 활성화 여부
BPDU Guard	BPDU Guard 활성화 여부. 기본적으로 선택되어 있지 않습니다. BPDU Guard 가 활성화되면 장치는 BPDU 를 수신하는 인터페이스를 종료하고 NMS 에 알립니다. 이러한 인터페이스는 네트워크 관리자가 수동으로만 복원할 수 있습니다.
Point-to-Point	활성화, 종료 및 자동 모드를 선택합니다. Auto mode: 이는 기본 자동 검사와 지점 간 링크 간의 연결 상태를 나타냅니다. Enabled mode: 이는 특정 포트가 지점 간 링크에 연결되어 있음을 나타냅니다. Shutdown mode: 이는 특정 포트가 지점 간 링크 연결에 실패했음을 나타냅니다.

2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

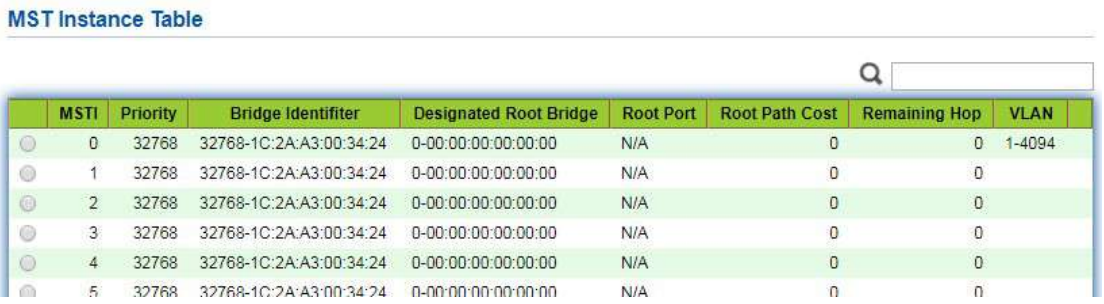
9.3 MST 인스턴스

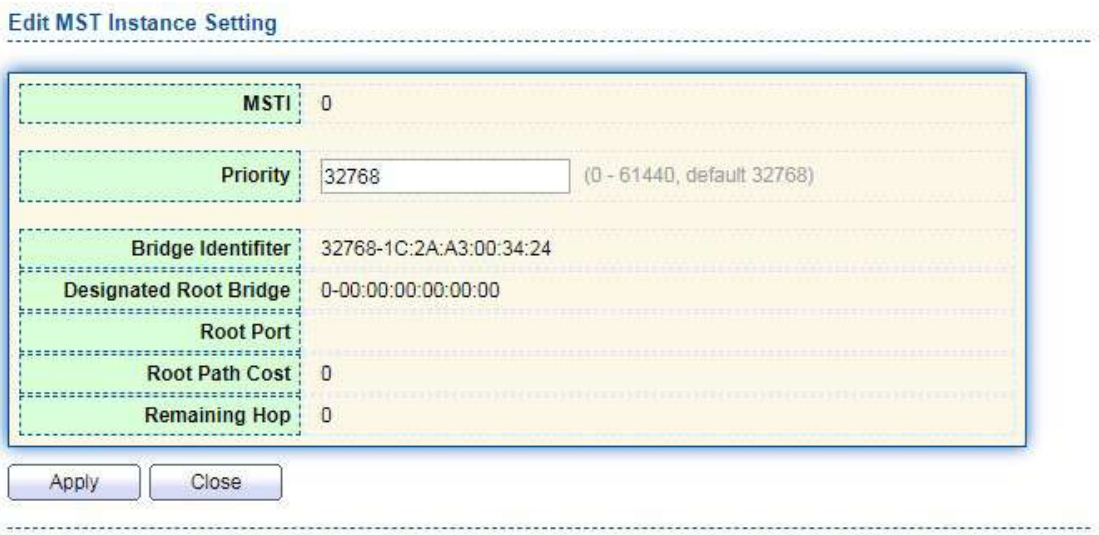
스위칭 네트워크는 MSTP 에 의해 여러 도메인으로 구분되며 각 도메인 내에 독립적인 스패닝 트리가 형성됩니다. 각각의 스패닝 트리를 MSTI(Multiple Spanning Tree Instance)라 하고, 각 도메인을 MST 영역(Multiple Spanning Tree Region)이라 부른다.

인스턴스는 통신 비용과 자원 활용률을 줄이는 VLAN 그룹입니다. 토폴로지를 통해 독립적으로 계산된 각 인스턴스는 로드 밸런싱을 수행할 수 있습니다. 동일한 토폴로지를 갖는 VLAN 은 동일한 인스턴스에 매핑될 수 있으며, 해당 MSTP 인스턴스의 포트 상태에 따라 전달됩니다.

간단히 말해서 지정된 MST 인스턴스에 매핑되면 하나 이상의 VLAN 이 한 번에 스패닝 트리에 배포됩니다.

1. 탐색 모음에서 "Spanning Tree > MST Instance"를 클릭하고 다음과 같이 구성할 선택한 스패닝 트리 인스턴스를 "Edit"합니다.





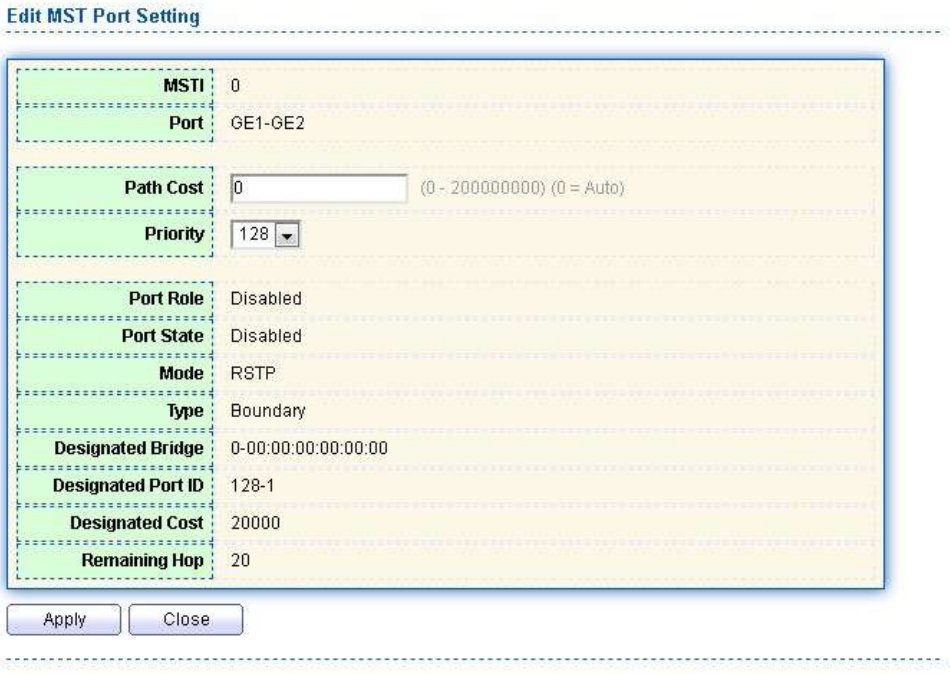
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
MSTI	Instance No. of spanning trees ranges from 0 to 15
VLAN	VLAN No. mapped from instances
Priority	Set the priority of a multiple of 4,096 for the specified instance, ranging from 0 to 65,535 with 32,768 as default.

2. 해당 구성 항목을 입력합니다.
3. “적용”을 선택하고 다음과 같이 마무리합니다.

9.4 MST 포트 설정

1. 네비게이션 바에서 “Spanning Tree > MST Port Setting”을 클릭하고 장치의 모든 포트 목록에서 수정할 포트를 선택한 후 “편집”을 클릭하여 다음과 같이 세부 구성 인터페이스로 들어갑니다.



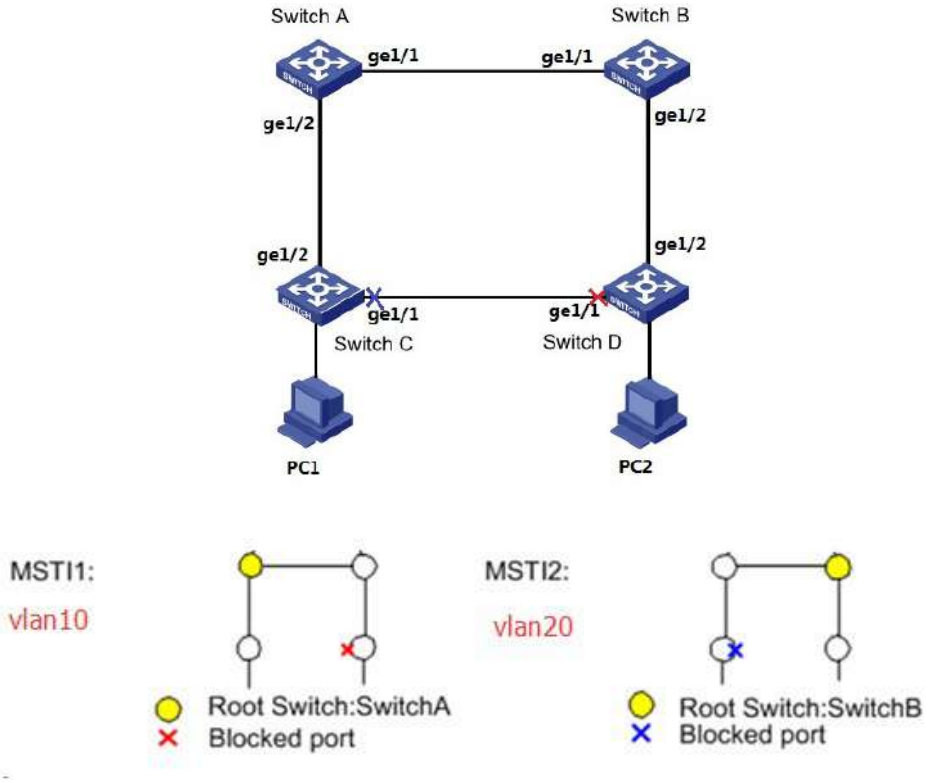
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
MSTI	왼쪽 상단의 드롭다운 상자를 통해 구성할 인스턴스를 선택합니다.
Port	사용자가 구성할 포트를 선택하세요.
Path Cost	인터페이스의 경로 비용 값을 입력합니다. 0~200,000,000 범위의 값으로 IEEE 802.1t 표준을 사용합니다.
Priority	더 높은 우선순위를 나타내는 작은 값으로 포트 우선순위를 선택하십시오. 인터페이스 우선순위는 지정된 MSTI 의 인터페이스 역할에 영향을 미칩니다. 다른 MSTI 에서 사용자는 동일한 인터페이스에 대한 우선순위를 구성할 수 있습니다. 결과적으로 다양한 VLAN 의 흐름이 물리적 링크를 따라 전달되어 VLAN 로드 공유를 달성할 수 있습니다. 설명: MSTP 는 인터페이스 역할을 다시 계산하고 우선 순위가 변경되면 해당 상태를 마이그레이션합니다.
Port Role	루트 포트에는 지정된 포트, 백업 포트, 비활성화된 포트 등 3 가지 유형이 있습니다.
Port State	폐기, 전달 및 비활성화의 3 가지 상태 포함
Mode	현재 STP 모드
Type	인스턴스의 포트 유형에는 경계 및 내부 포트가 포함됩니다.

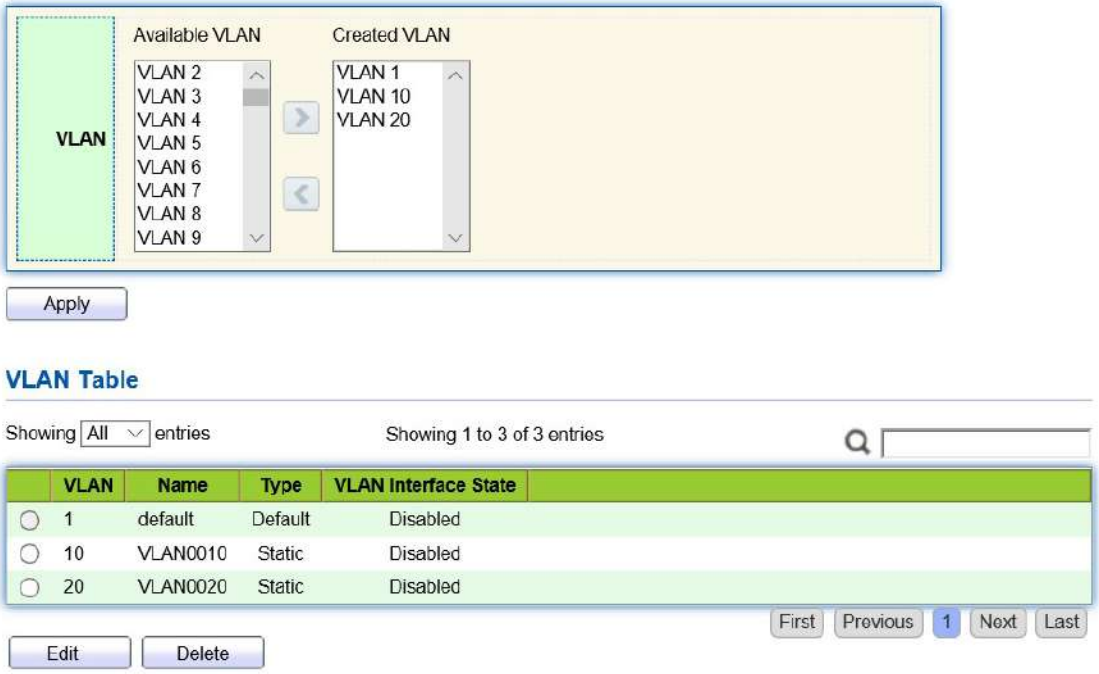
2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

MSTP 기능 구성의 예:

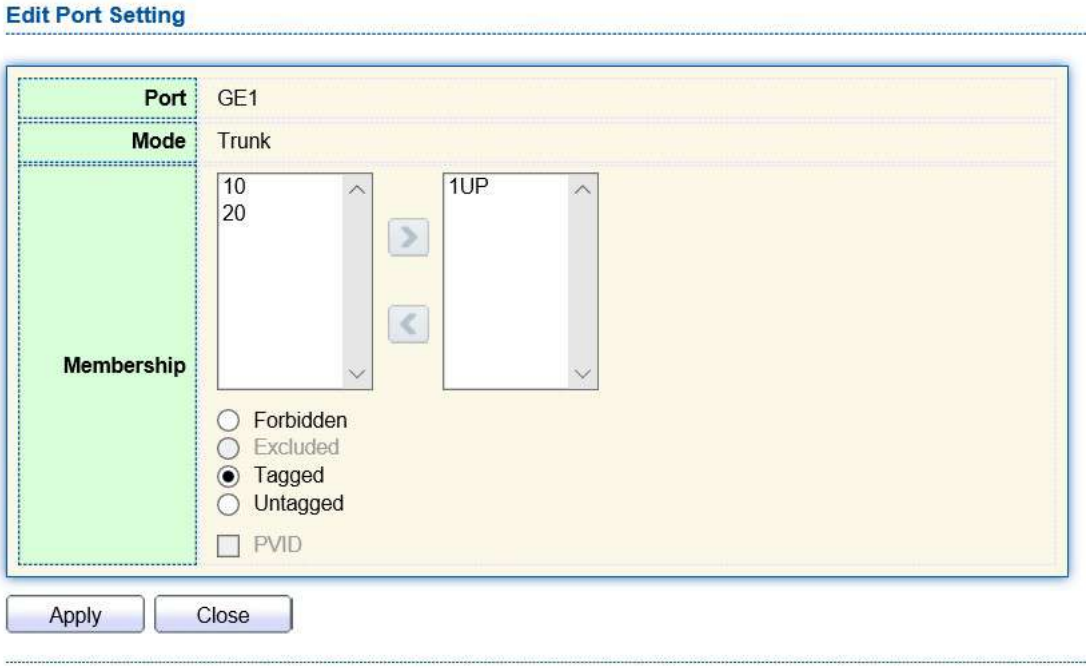
스위치 A, B, C 및 D 는 모두 VLAN10 과 20 의 로드를 공유하기 위해 인스턴스를 도입하는 MSTP 를 실행합니다. MSTP 는 VLAN 매핑 테이블을 설정하여 VLAN 을 스패닝 트리 인스턴스와 연결하고 인스턴스 1 의 VLAN10 과 인스턴스 2 의 VLAN20 을 매핑할 수 있습니다.



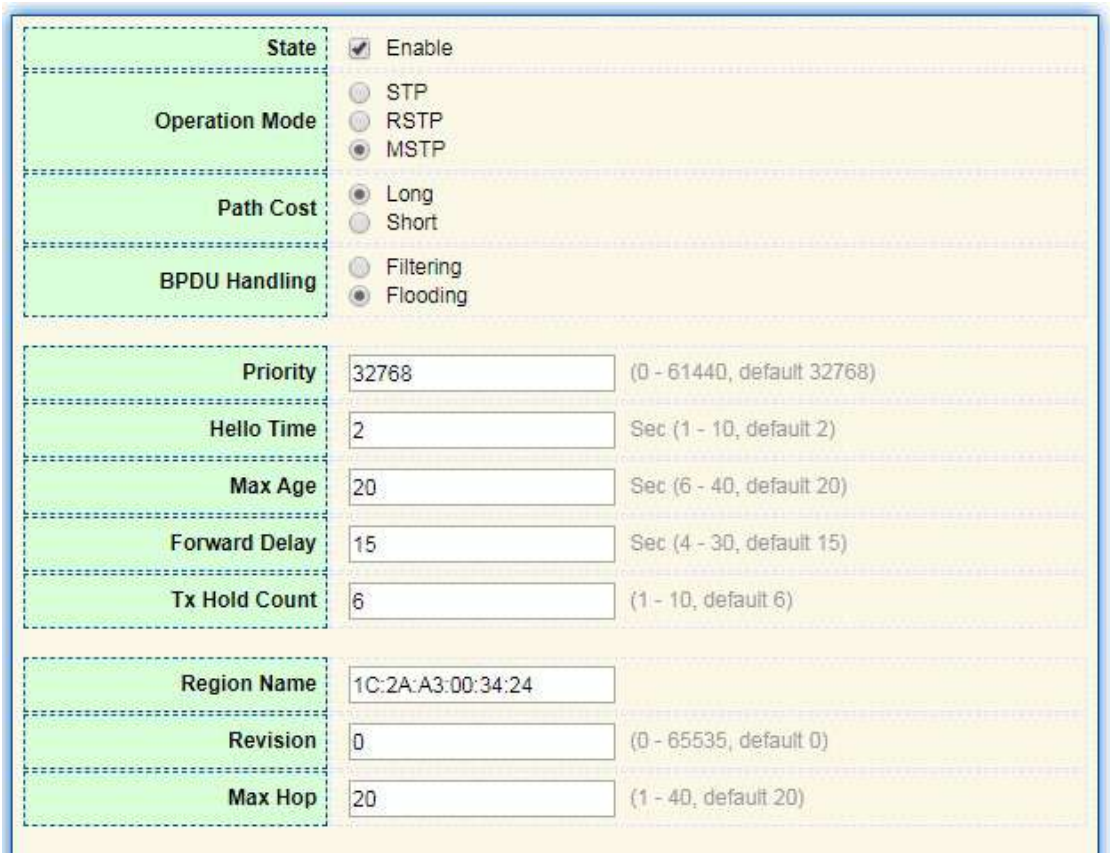
1. 스위치 A, B, C 및 D 는 VLAN10 및 20 을 생성하여 링에 있는 장치의 L2 전달 기능을 구성합니다. 탐색 표시줄에서 "VLAN > VLAN > VLAN 생성"을 클릭하고 해당 구성을 입력합니다. “적용”을 선택하고 다음과 같이 마무리합니다.



2. VLAN 은 스위치 포트 수신 루프에 추가됩니다. 탐색 모음에서 “VLAN > VLAN > Membership”을 클릭하고 구성할 링 포트를 선택한 다음 VLAN10 과 20 을 오른쪽 상자로 이동하고 “Tagged”로 표시합니다. "적용"하고 완료합니다.



3. 탐색 모음에서 “Spanning Tree > 프로퍼티”을 클릭하고 다음과 같이 MSTP 모드를 선택합니다.



4. 인스턴스 MSTI1 과 MSTI2 간의 VLAN 매핑을 구성합니다. “Spanning Tree > MST Instance”를 클릭하여 해당 매개변수를 입력하고 다음과 같이 “Add”합니다.

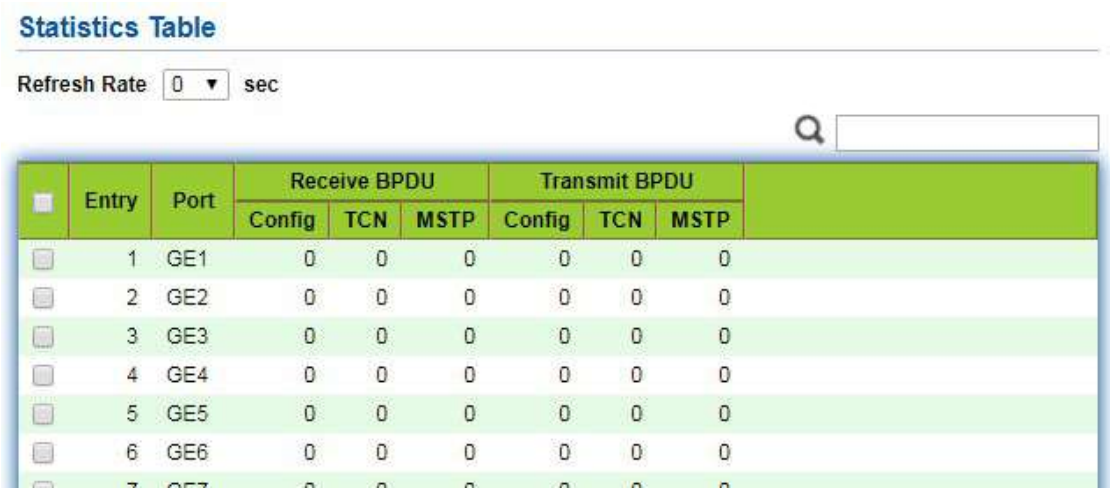
Note:

- Switch A 를 구성하기 전에 MSTI1 의 우선순위를 0 으로, MSTI2 의 우선순위를 4,096 으로 설정하세요.
- 스위치 B 를 구성하기 전에 MSTI1 의 우선순위를 4,096 으로, MSTI2 의 우선순위를 0 으로 설정하세요.
- 우선순위는 4,096 의 배수여야 합니다.

5. 스위치 B 는 도메인에서 MSTI2 의 루트 브리지 역할과 MSTI1 의 백업 루트 브리지 역할을 합니다. 가이드는 5 를 참조하십시오.
6. 트리 모양의 네트워크는 루프를 제거합니다.

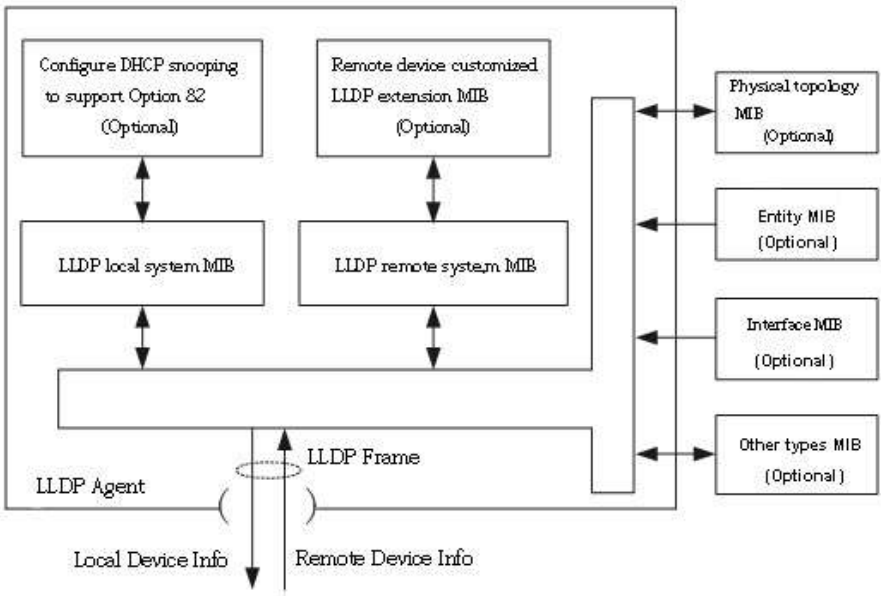
9.5 통계

1. 탐색 모음에서 " Spanning Tree > Statistics "를 클릭하면 다음과 같이 항목 포트 통계가 표시됩니다.



10 Discovery

LLDP(링크 계층 검색 프로토콜)는 IEEE 802.1ab 에 정의되어 있습니다. 로컬 네트워크 장치의 관리 주소, 장치, 인터페이스 식별 정보 등의 정보를 통합하여 주변 장치로 전송하는 표준 L2 탐색 방법입니다. 정보를 받은 후 NMS 쿼리 및 링크 통신 판단을 위해 표준 MIB(Management Information Base) 형식으로 저장합니다.
또한 정보를 통합하고 자체 원격 장치로 전송할 수도 있습니다. 로컬 네트워크 장치가 수신한 정보는 MIB 형태로 보관됩니다. 다음은 작동 방식을 보여줍니다.
LLDP 원리의 블록 다이어그램



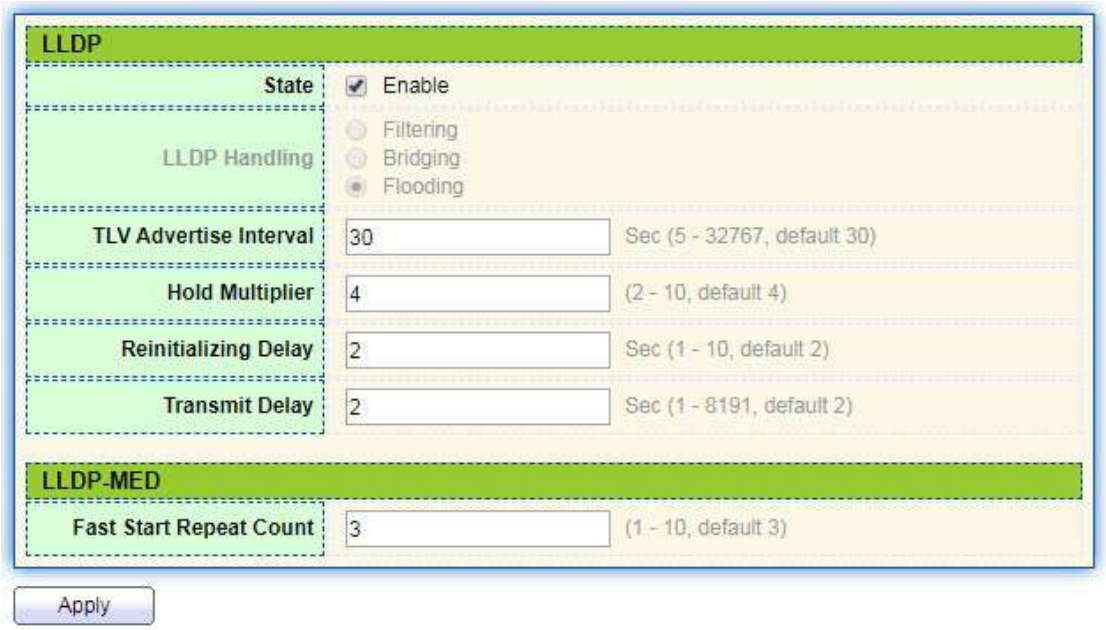
LLDP 는 다음을 기반으로 실현됩니다.

- LLDP 모듈은 LLDP 에이전트와 물리적 토폴로지, 엔터티, 인터페이스 및 기타 유형의 MIB 간의 상호 작용을 통해 로컬 시스템 MIB 뿐만 아니라 사용자 정의 확장 MIB 를 업데이트합니다.
- 로컬 네트워크 장치의 정보를 LLDP 프레임으로 캡슐화하여 원격 장치로 전송합니다.
- LLDP 원격 시스템 MIB 및 사용자 정의 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 하는 LLDP-MED 를 사용하면 다른 장치를 확장할 수 있습니다. 네트워크 장치에서 확인된 정보는 장애 분석을 용이하게 하고 관리 시스템의 네트워크 토폴로지에 대한 정확한 이해를 심화시킵니다.

10.1 LLDP

1. 다음과 같이 네비게이션 바에서 “Discovery > LLDP > 프로퍼티”를 클릭하세요.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
State	LLDP 활성화 또는 비활성화
LLDP Handling	LLDP 메시지는 LLDP 를 비활성화할 때 "필터링", "브리징" 및 "플러딩"을 통해 처리됩니다.
TLV Advertise Interval	기본적으로 30 초 범위는 5~32,768 초입니다.
Hold Multiplier	기본적으로 4 가 포함된 전송주기 제품은 2~10 입니다. 전송주기 * 제품은 65,535 이하여야 합니다.
Reinitializing Delay	기본적으로 2 초 범위는 1~10 초입니다.
Transmit Delay	기본적으로 2 초 범위는 1~8,191 초입니다.
Fast Start Repeat Count	1~10 초 범위의 LLDP-MED 포트는 기본적으로 3 초입니다.

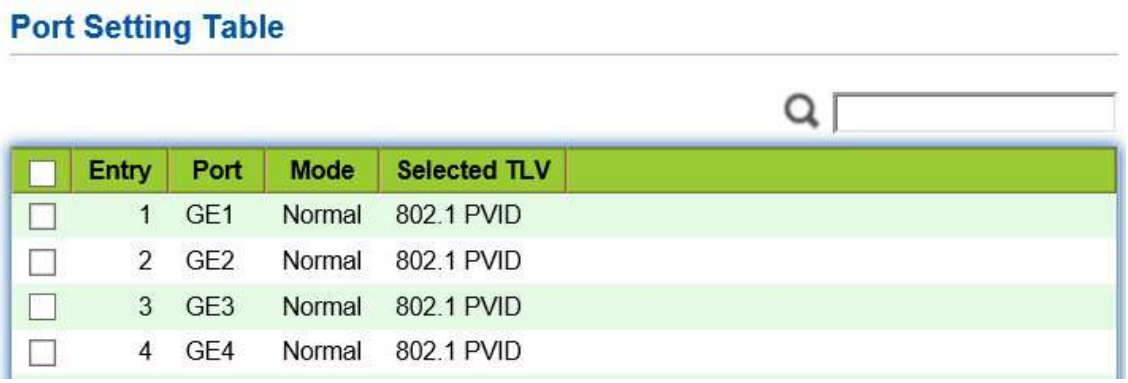
LLDPDU(LLDP Data Unit)로 캡슐화된 이더넷 메시지는 LLDP 메시지로 인식됩니다. 각 TLV 는 지정된 정보와 함께 전달되는 LLDPDU 단위입니다.

2. 해당 구성 항목을 입력합니다.

3. ""적용"하고 마무리합니다.

10.2 포트 설정

1. 다음과 같이 탐색 표시줄에서 "Discovery > LLDP > Port Setting"을 클릭합니다.

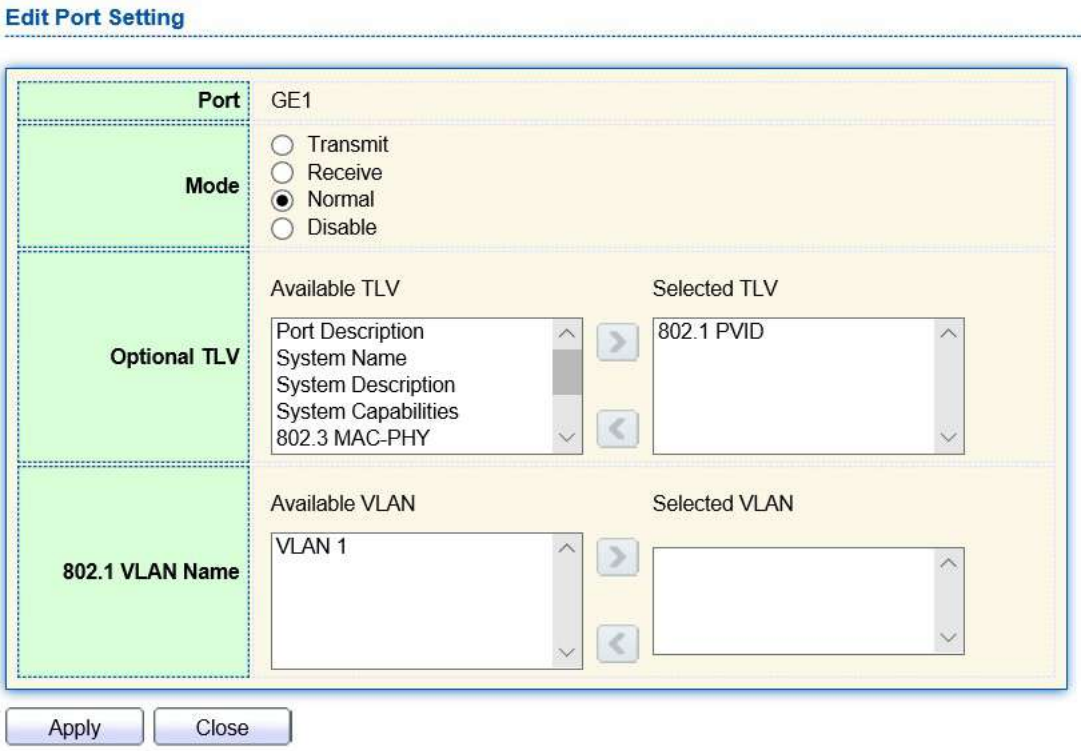


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
Mode	LLDP 모드에는 Transmit, Receive, Normal, Disable 가 포함되며 기본값은 Normal 입니다. Transmit: LLDP 메시지만 전송합니다. Receive: LLDP 메시지만 수신합니다. Normal: LLDP 메시지 전송 및 수신 Disable: LLDP 메시지를 전송하거나 수신하지 않습니다.
Selected TLV	선택된 TLV 및 VLAN 정보

LLDP 는 4 가지 패턴으로 작동할 수 있습니다. Transmit: LLDP 메시지만 전송합니다. Receive: LLDP 메시지만 수신합니다. Normal: LLDP 메시지 전송 및 수신 Disable: LLDP 메시지를 전송하거나 수신하지 않습니다.

2. 해당 포트를 확인하고 포트 구성을 “편집”하세요. “적용”을 선택하고 다음과 같이 마무리합니다.



인터페이스 데이터는 다음과 같습니다.

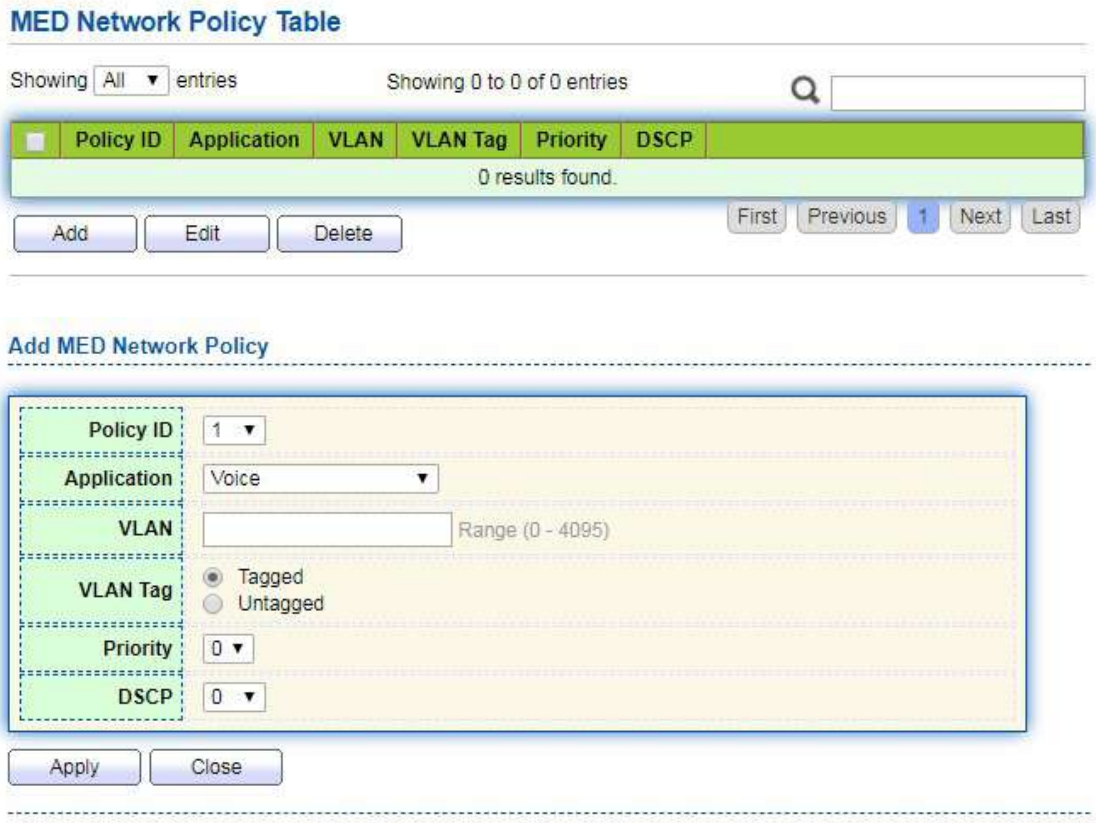
설정 항목	설명
Port	포트 목록
Mode	LLDP 모드에는 Transmit, Receive, Normal, Disable 가 포함되며 기본값은 Normal 입니다. Transmit: LLDP 메시지만 전송합니다. Receive: LLDP 메시지만 수신합니다. Normal: LLDP 메시지 전송 및 수신 Disable: LLDP 메시지를 전송하거나 수신하지 않습니다.
Optional TLV	TLV 및 VLAN 정보를 선택하세요.
802.1 VLAN Name	VLAN 이름을 선택하세요.

10.3 MED 네트워크 정책

MED 는 IEEE 802.1ab 를 기반으로 합니다. LLDP 는 다른 조직에서 확장할 수 있는 IEEE 의 이웃 검색 프로토콜입니다. 스위치 및 무선 액세스 포인트와 같은 네트워크 장치에서 식별된 정보는 결함 분석에 도움이 되며 관리 시스템이 네트워크 토폴로지를 정확하게 이해할 수 있도록 해줍니다.

1. 다음과 같이 탐색 표시줄에서 “Discovery > LLDP > MED Network Policy”를

클릭합니다.

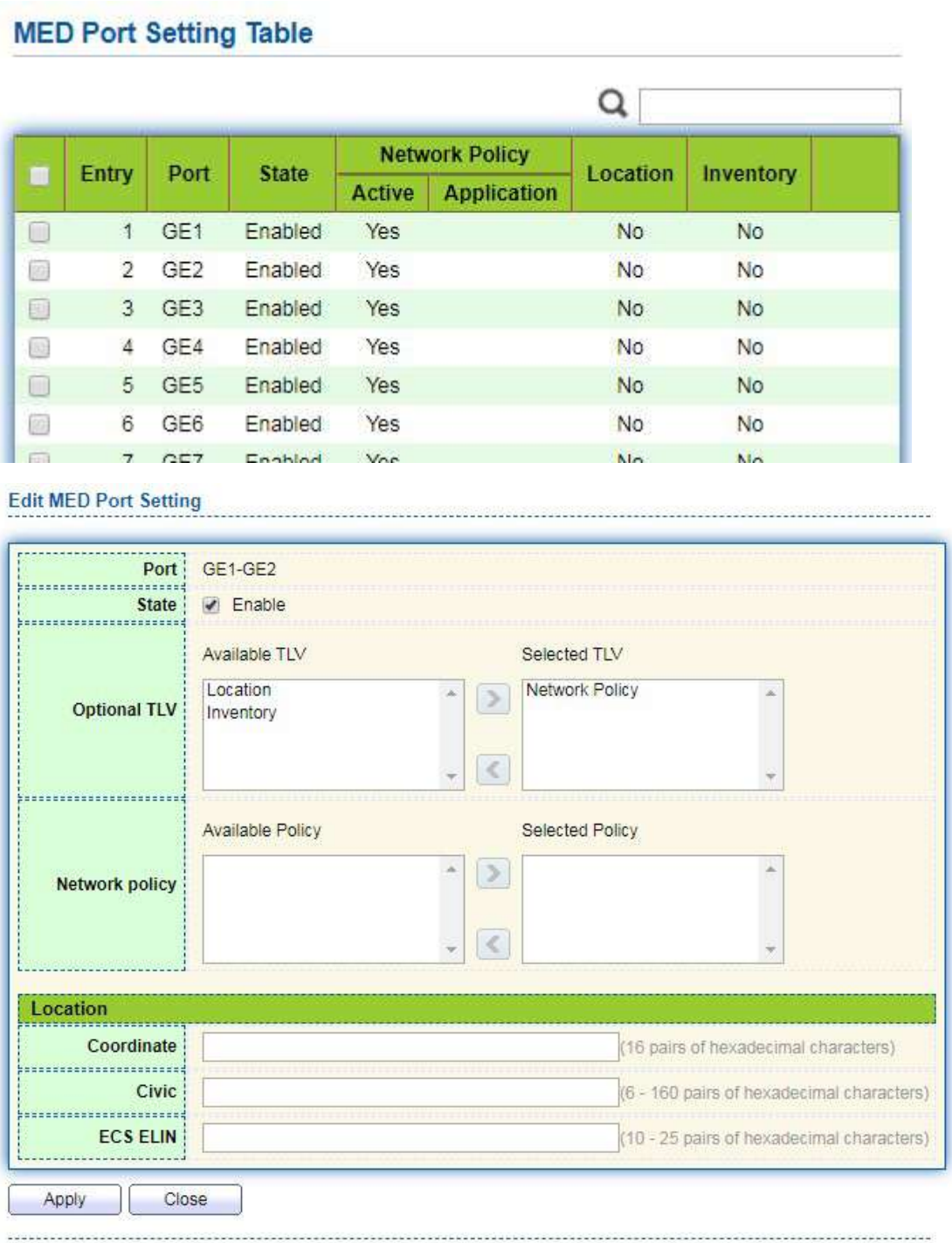


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Policy ID	정책 ID 번호
Application	네트워크 정책 TLV 구성 및 게시
VLAN	VLAN 번호
VLAN Tag	VLAN 모드, 태그 지정 또는 태그 없음 옵션
Priority	서비스를 위한 CoS
DSCP	서비스용 DSCP

10.4 MED 포트 설정

1. 다음과 같이 탐색 표시줄에서 “Discovery > LLDP > MED Port Setting”을 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Entry	MED 포트 설정 일련번호
Port	포트 목록
State	포트 활성화 상태
Network Policy	네트워크 정책 TLV 구성 및 게시

Location	위치 TLV 구성 및 게시
Inventory	인벤토리 TLV 구성 및 게시

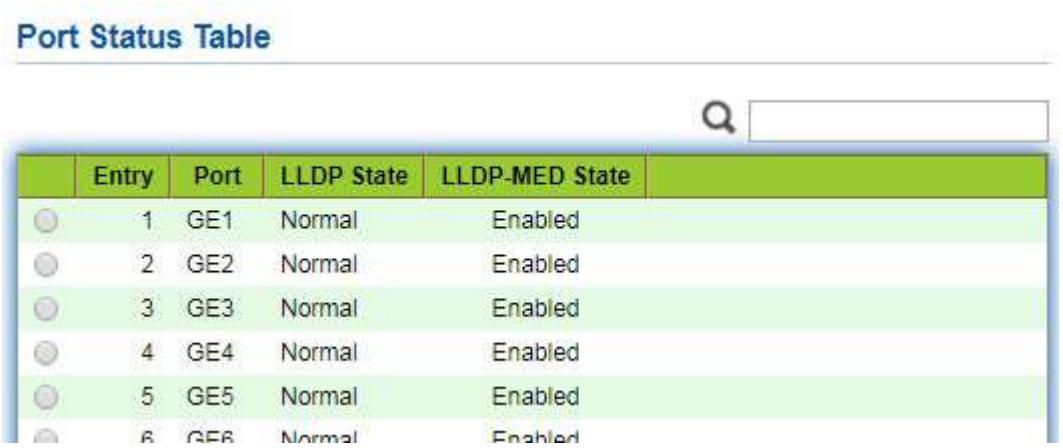
10.5 패킷 보기

1. 다음과 같이 네비게이션 바에서 “Discovery > LLDP > Packet View”를 클릭합니다.

10.6 로컬 정보

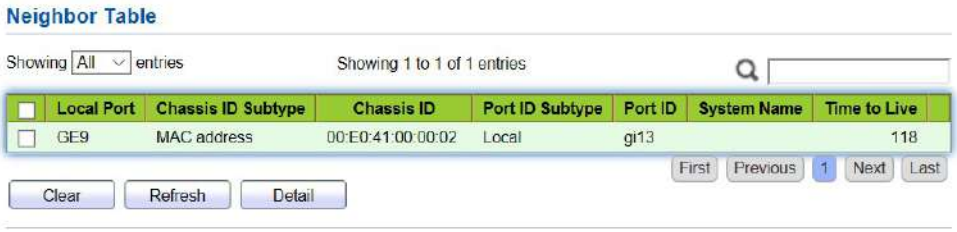
1. 다음과 같이 네비게이션 바에서 “Discovery > LLDP > Local Information”을 클릭하세요.

2. 다음과 같이 네비게이션 바에서 “Discovery > LLDP > Local Information”을 클릭하세요.



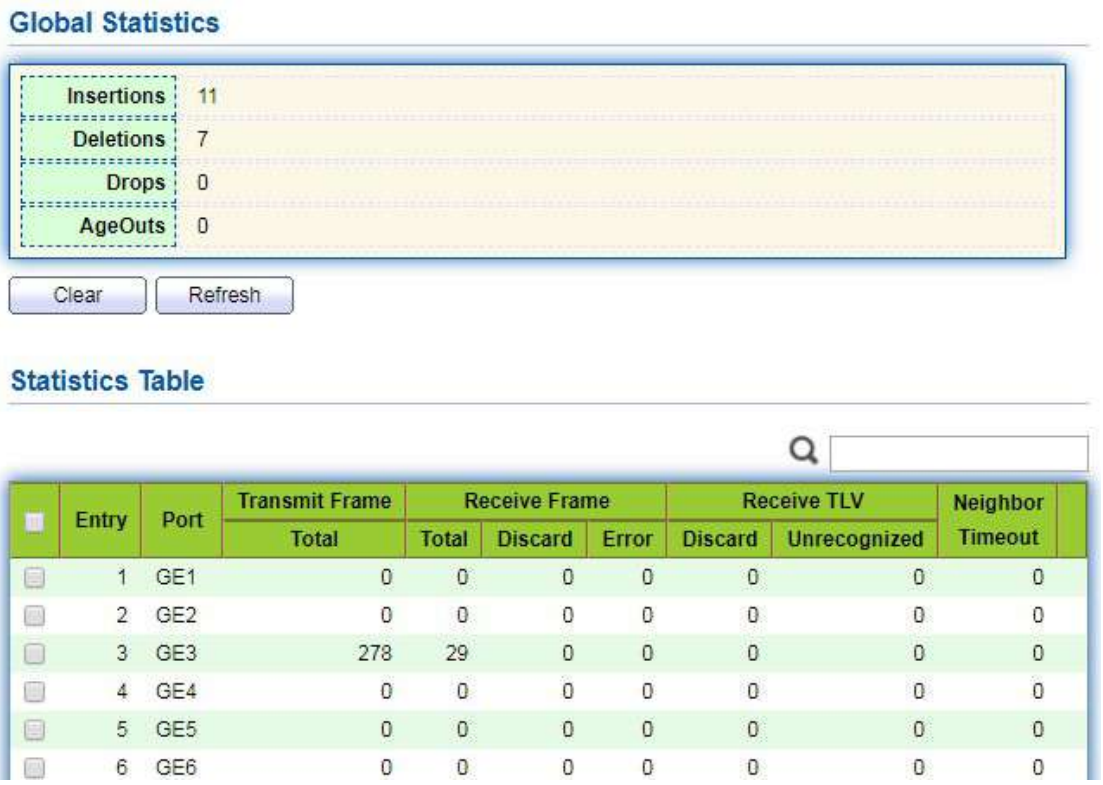
10.7 Neighbor

1. 다음과 같이 네비게이션 바에서 “Discovery > LLDP > Neighbor”를 클릭하세요.



10.8 Statistics

1. 다음과 같이 네비게이션 바에서 “Discovery > LLDP > Statistics”를 클릭하세요.



11 DHCP

DHCP 서버 간략한 소개

네트워크 규모가 확장되고 네트워크 복잡성이 개선됨에 따라 네트워크 구성이 점점 더 복잡해지고 있습니다. 컴퓨터 위치가 변경되고(예: 휴대용 컴퓨터 또는 무선 네트워크) 컴퓨터 수가 할당할 수 있는 IP 주소를 초과합니다.

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

일반적인 DHCP 애플리케이션에는 그림 1-1 에 표시된 것처럼 일반적으로 DHCP 서버와 여러 클라이언트(예: PC 및 노트북)가 포함됩니다.

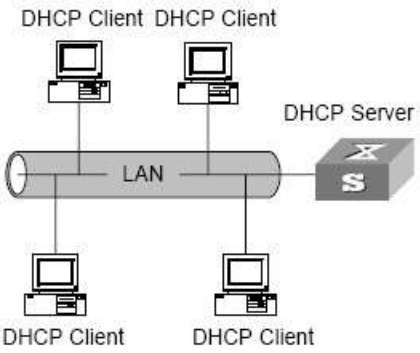


Figure 1-1. In a typical application of DHCP

DHCP 의 IP 주소 할당

IP 주소 할당 전략

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

- Manual address assignment: 관리자는 몇 가지 특정 클라이언트(예: WWW 서버)에 대해 고정 IP 주소를 바인딩합니다. 구성된 고정 IP 주소를 DHCP 를 통해 클라이언트에 보냅니다.
- Automatic address assignment: DHCP 는 무제한 임대 기간으로 IP 주소를 클라이언트에 할당합니다.
- Dynamic address assignment: DHCP 는 유효 기간이 있는 IP 주소를 클라이언트에 할당하며, 클라이언트는 서비스 수명 만료 후 주소를 다시 신청해야 합니다. 대부분의 클라이언트는 이러한 동적 주소 할당을 받습니다.

동적 IP 주소 획득 프로세스

그림 2-1 은 DHCP 클라이언트와 DHCP 서버 간의 메시지 상호작용 과정을 보여줍니다.

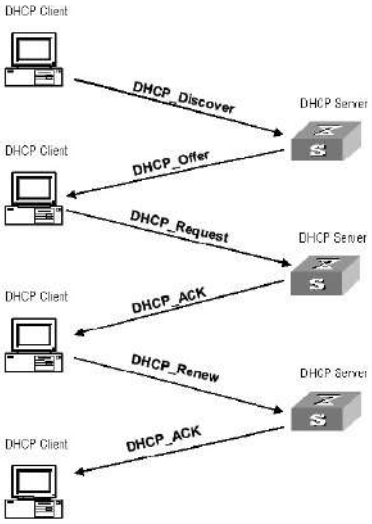


Figure 2-1. Interaction process

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

(1) DHCP 클라이언트가 처음으로 네트워크에 로그인합니다.

DHCP 클라이언트가 네트워크에 처음 로그인할 때 주로 4 단계를 거쳐 DHCP 서버와 연결을 설정합니다.

- The discovery phase: DHCP 클라이언트가 DHCP 서버를 찾는 단계입니다. 클라이언트는 브로드캐스트 모드에서 DHCP 검색 메시지를 보내고 DHCP 서버만 응답합니다.
- The stage of providing IP address: 즉, DHCP 서버가 IP 주소를 제공하는 단계입니다. DHCP 서버는 클라이언트로부터 DHCP Discover 메시지를 수신한 후 IP 주소 풀에서 할당되지 않은 IP 주소를 선택하여 클라이언트에 할당하고, 임대된 IP 주소 및 기타 설정이 포함된 DHCP Offer 메시지를 클라이언트에 보냅니다.
- The selection stage: DHCP 클라이언트가 IP 주소를 선택하는 단계입니다. 두 개 이상의 DHCP 서버가 클라이언트에게 DHCP Offer 메시지를 보내는 경우, 클라이언트는 처음 수신한 DHCP Offer 메시지만 수락한 후, 각 DHCP 서버에 브로드캐스트하여 DHCP 요청 메시지에 응답합니다. 해당 정보에는 선택한 DHCP 서버에 IP 주소를 요청하는 내용이 포함되어 있습니다.
- The confirmation stage: DHCP 서버가 제공된 IP 주소를 확인하는 단계입니다. DHCP 서버는 DHCP 클라이언트가 응답한 DHCP 요청 메시지를 받으면 클라이언트가 제공한 IP 주소와 기타 설정이 포함된 dhcp-ack 확인 메시지를 보냅니다. 그렇지 않으면 주소를 클라이언트에 할당할 수 없음을 나타내는 dhcp-nak 메시지가 반환됩니다. 서버가 반환한 dhcp-ack 확인 메시지를 받은 후 클라이언트는 주소 감지를 위해 브로드캐스트 모드로 ARP(대상 주소는 할당된 주소)를 보냅니다. 지정된

시간 내에 응답이 수신되지 않으면 클라이언트는 이 주소를 사용합니다.

(2) DHCP 클라이언트가 네트워크에 다시 로그온합니다.

DHCP 클라이언트가 네트워크에 다시 로그인할 때 주로 다음 단계를 통해 DHCP 서버와 연결을 설정합니다.

- DHCP 클라이언트가 처음으로 네트워크에 올바르게 로그인한 후 다시 네트워크에 로그인한 후에는 마지막에 할당한 IP 주소가 포함된 DHCP 요청 메시지만 브로드캐스팅하면 되며 DHCP 클라이언트를 보낼 필요는 없습니다. 메시지를 다시 발견하세요.
- DHCP 요청 메시지를 수신한 후, 클라이언트가 요청한 주소가 할당되지 않은 경우 dhcp-ack 확인 메시지를 반환하여 DHCP 클라이언트에게 원래 IP 주소를 계속 사용하도록 알립니다.
- IP 주소를 DHCP 클라이언트에 할당할 수 없는 경우(예: 다른 클라이언트에 할당된 경우) DHCP 서버는 dhcp-nak 메시지를 반환합니다. 메시지를 받은 후 클라이언트는 DHCP Discover 메시지를 다시 전송하여 새 IP 주소를 요청합니다.

(3) DHCP 클라이언트는 IP 주소의 임대 유효 기간을 연장합니다.

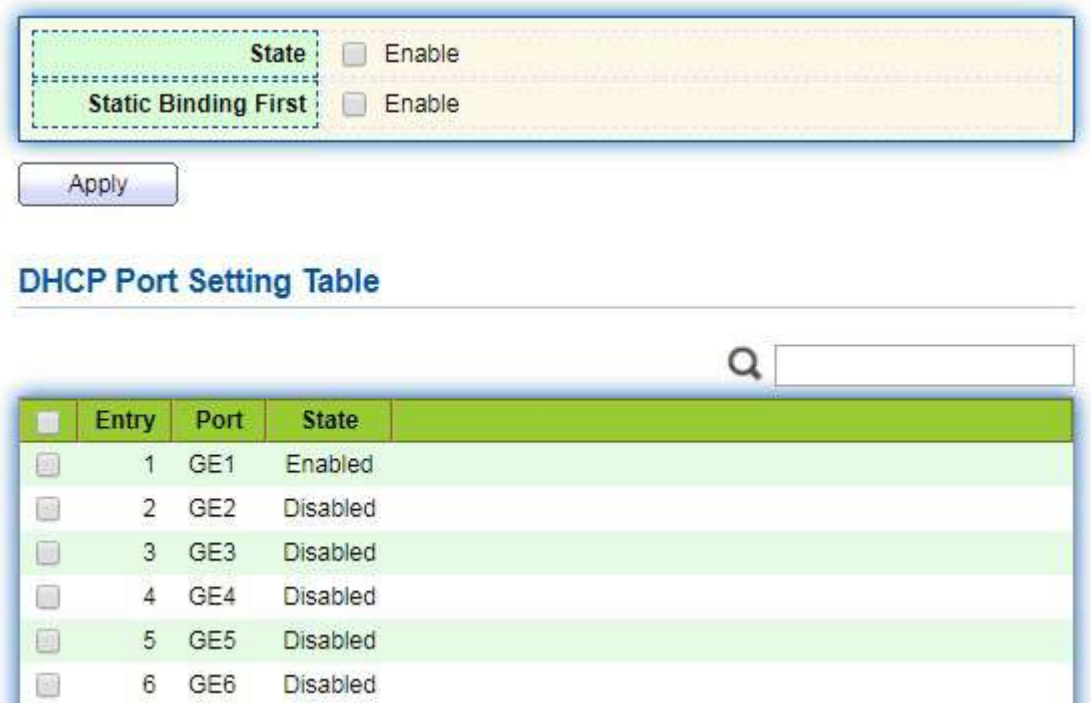
DHCP 서버가 클라이언트에 할당하는 동적 IP 주소에는 일반적으로 특정 임대 기간이 있습니다. 만료 후 서버는 IP 주소를 다시 가져옵니다. DHCP 클라이언트가 해당 주소를 계속 사용하려면 IP 임대를 업데이트해야 합니다.

실제로 DHCP 클라이언트는 IP 임대 기간이 절반에 도달하면 기본적으로 DHCP 요청 메시지를 DHCP 서버로 보내 IP 임대 업데이트를 완료합니다. IP 주소가 유효하면 DHCP 서버는 dhcp-ack 메시지에 응답하여 DHCP 클라이언트에게 새로운 임대가 획득되었음을 알립니다.

11.1 프로퍼티

DHCP 전역 및 정적 바인딩 구성

1. 다음과 같이 탐색 표시줄에서 “DHCP > 프로퍼티”을 클릭합니다.



2. “DHCP > 프로퍼티”을 클릭하고, 포트를 선택하고 다음과 같이 “편집”을 클릭하세요.

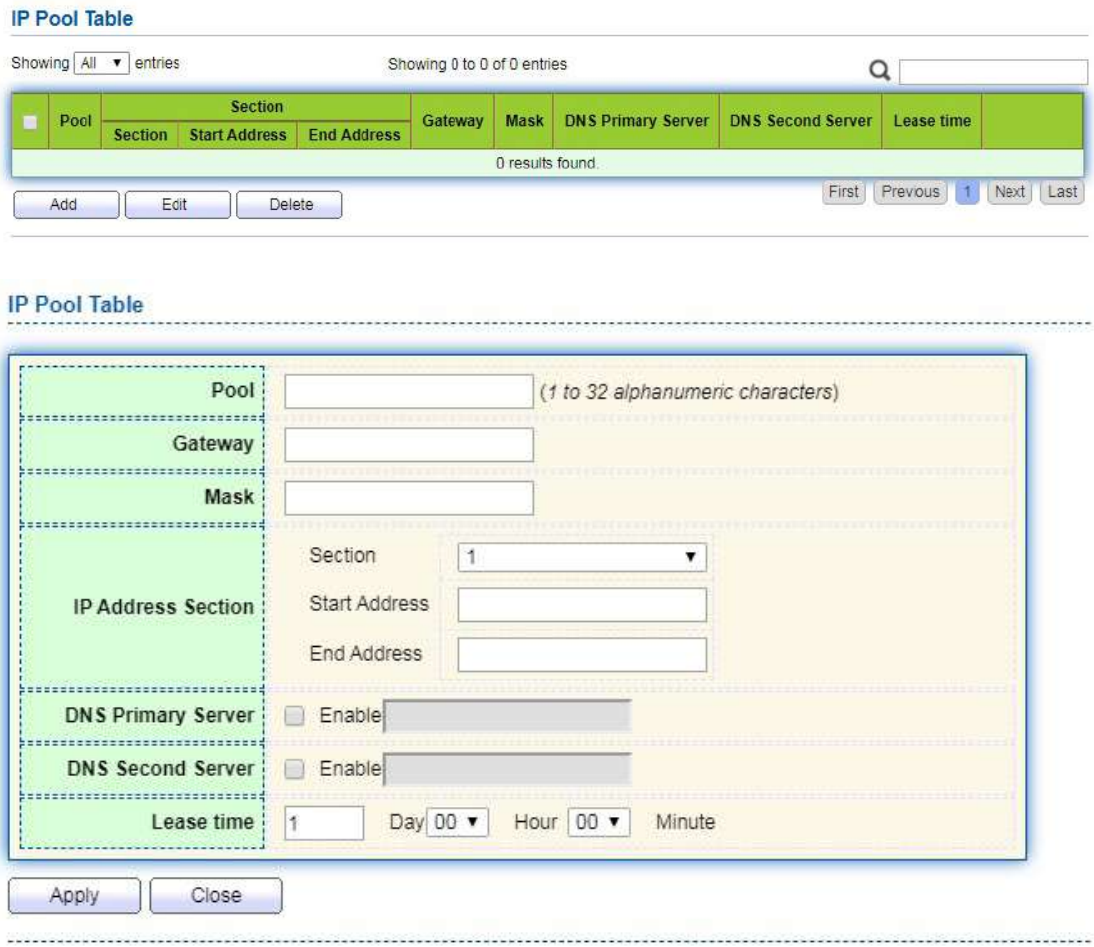
Note:

- DHCP 서버 또는 DHCP 릴레이 모드를 활성화합니다. 포트에서 이 기능을 활성화해야 합니다.

11.2 IP 풀 설정

DHCP IP 풀 구성

1. “DHCP > IP Pool Setting”을 클릭하고, “추가”를 클릭하여 다음과 같이 IP 풀을 추가합니다.



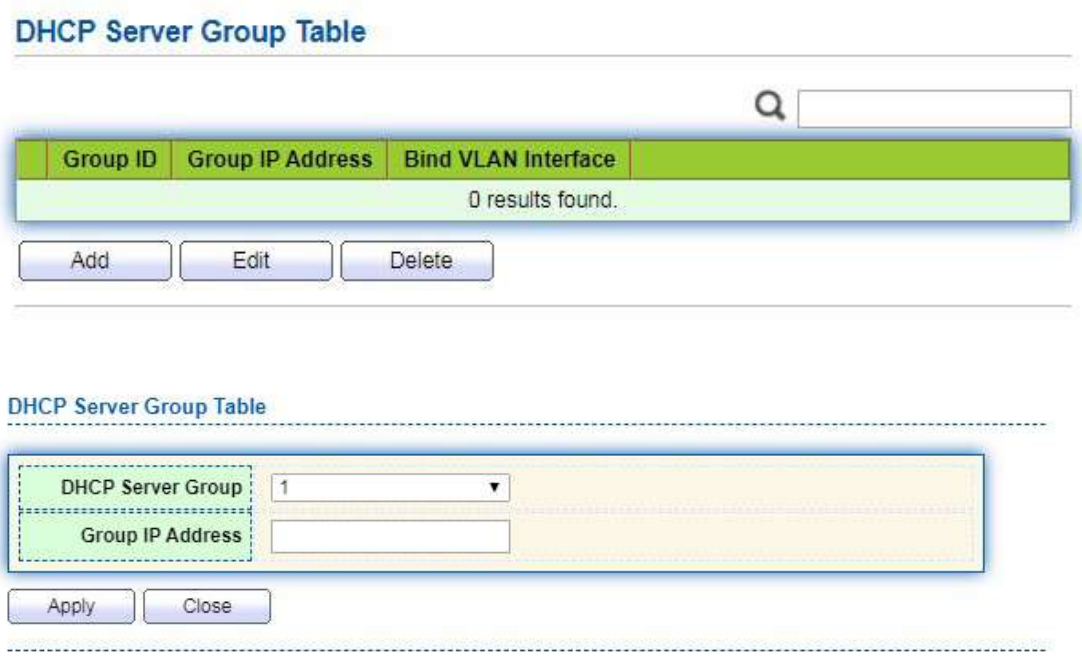
Note:

- 시작 주소와 끝 주소는 구성할 수 없거나 게이트웨이 주소를 포함할 수 없습니다.

11.3 VLAN IF 주소 그룹 설정

서버 그룹 구성

1. “DHCP > VLAN IF Address Group Setting”을 클릭하고 DHCP 서버 그룹 테이블을 입력한 후 “추가”를 클릭하여 다음과 같이 서버 그룹을 구성합니다.



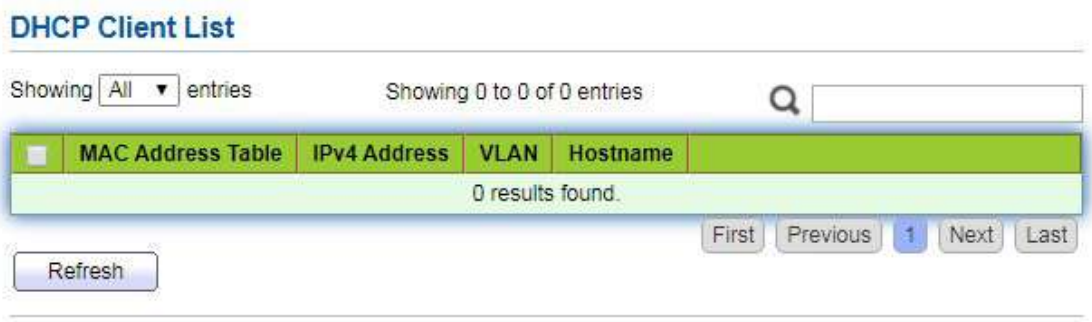
VLAN 인터페이스 및 서버 그룹 바인딩 구성

1. “DHCP > VLAN IF Address Group Setting”을 클릭하고 VLAN 인터페이스 주소 풀 테이블을 입력한 후 인터페이스와 서버 그룹을 선택하고 다음과 같이 “적용”을 클릭합니다.

11.4 클라이언트 리스트

클라이언트 리스트 정보

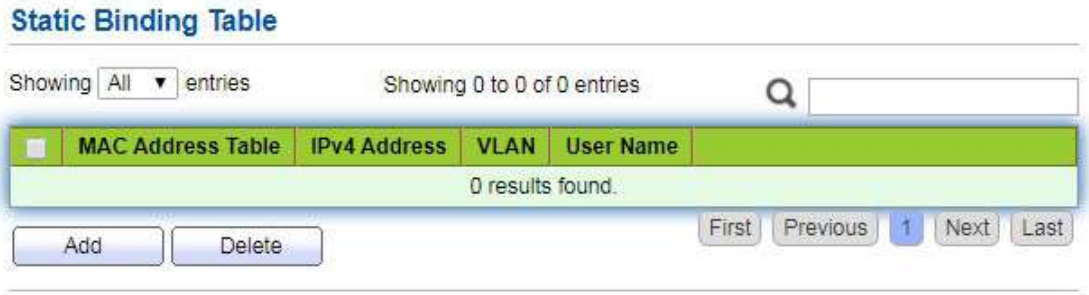
1. “DHCP > Client List”을 클릭하고, 다음과 같이 DHCP 클라이언트 목록을 입력하세요.



11.5 클라이언트 정적 바인딩 테이블

고정 IP 주소 할당 구성

1. “DHCP > Client Static Binding Table”을 클릭하고 다음과 같이 정적 바인딩 테이블을 입력한 후 “추가”를 클릭합니다.



Note:

- 고정 바인딩의 IP 구성은 IP 주소 할당 범위 내에 있어야 합니다.

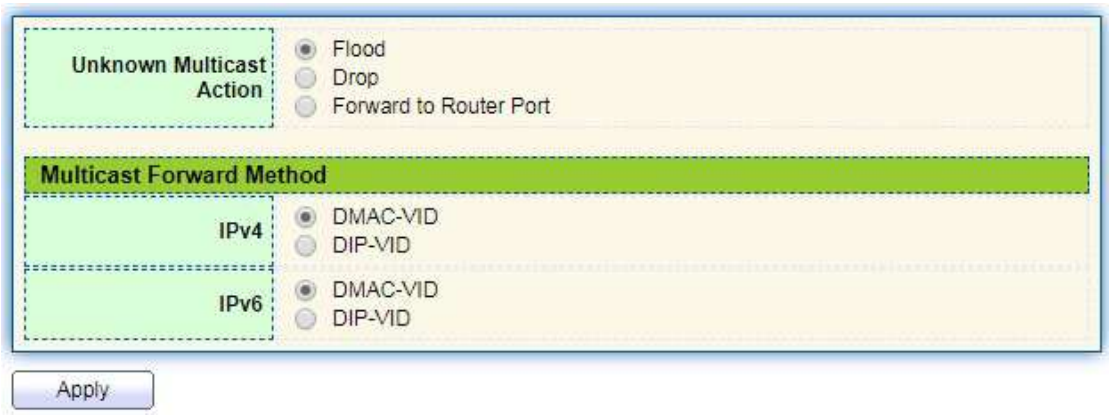
12 멀티캐스트

12.1 일반

12.1.1 프로퍼티

1. 다음과 같이 네비게이션 바에서 “Multicast > General > 프로퍼티 ”을

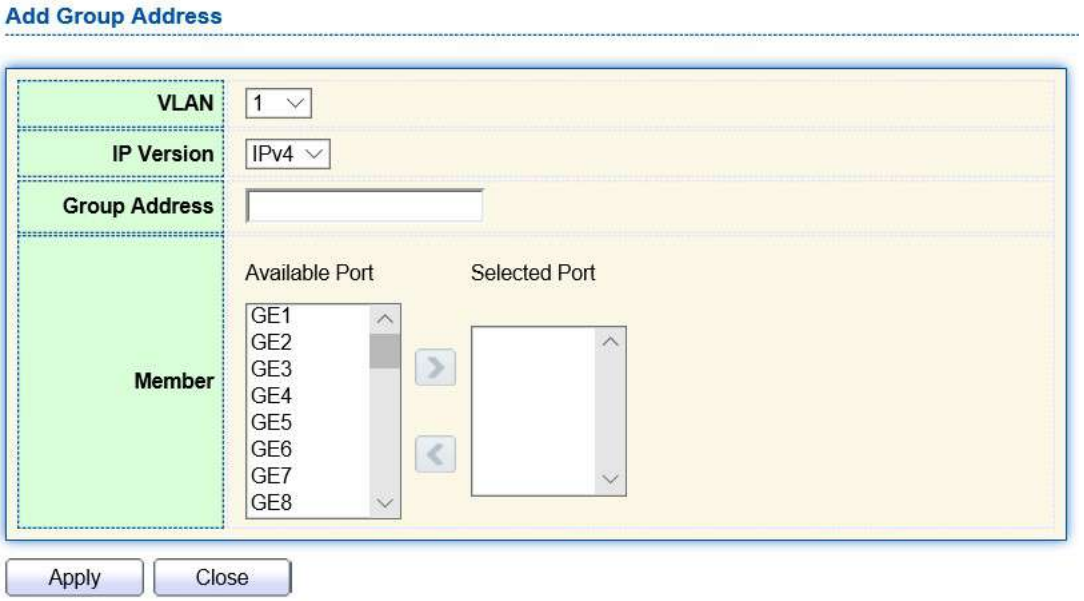
클릭하세요.



12.1.2 그룹 주소

이전 멀티캐스트 요청 모드에 따르면 멀티캐스트 라우터는 서로 다른 VLAN 의 사용자가 동일한 멀티캐스트 그룹을 요청할 때 수신기가 포함된 각 VLAN 에 데이터를 복사하여 전달하므로 대역폭이 많이 낭비됩니다. IGMP 스누핑은 스위치 포트의 서로 다른 사용자를 동일한 멀티캐스트 VLAN 에 연결하여 멀티캐스트 데이터를 수신함으로써 멀티캐스트 VLAN 을 구성합니다. 이러한 방식으로 멀티캐스트 흐름은 멀티캐스트 VLAN 내에서만 전송될 수 있으므로 대역폭이 절약됩니다. 또한 멀티캐스트 VLAN 은 사용자 VLAN 과 완전히 분리되어 있으므로 보안과 대역폭이 보장됩니다.

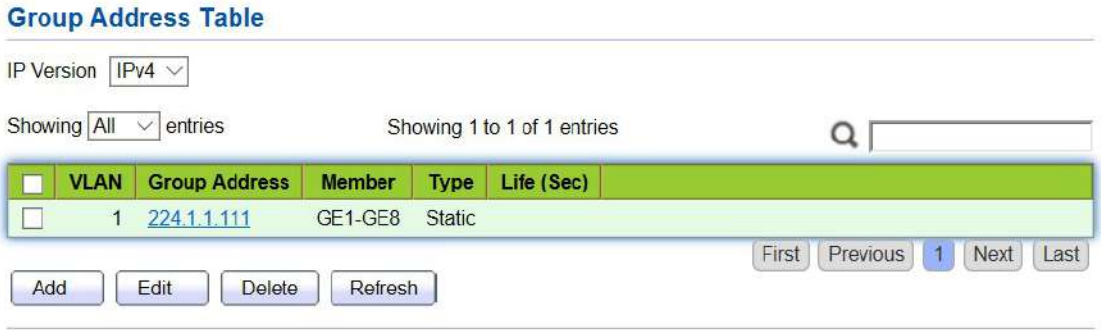
1. “Multicast > Group Address”를 클릭하고 새 정적 멀티캐스트 항목을 “추가”한 다음 기존 항목을 다음과 같이 “편집”합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	멀티캐스트 그룹이 속한 VLAN ID 입니다. 드롭다운하여 기존 VLAN 을 선택합니다.
IP Version	v4 또는 v6 이 멀티캐스트 IP 주소 버전인지 여부
Multicast Address	멀티캐스트 주소를 입력하세요
Member	멀티캐스트 구성원 추가

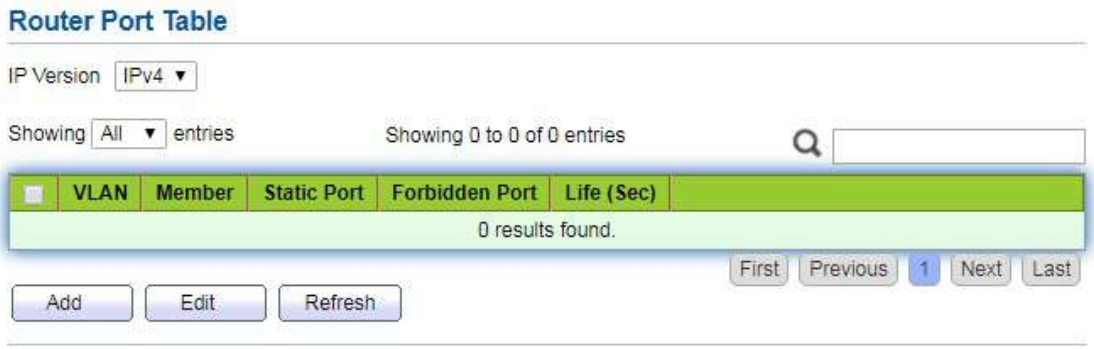
2. 해당 구성 항목을 입력합니다.
3. “적용”을 선택하고 다음과 같이 마무리합니다.



12.1.3 라우터 포트

멀티캐스트 라우터 포트 구성 및 보기

1. 다음과 같이 네비게이션 바에서 “Multicast > General > Router Port ”를 클릭하세요.



12.1.4 Forward All

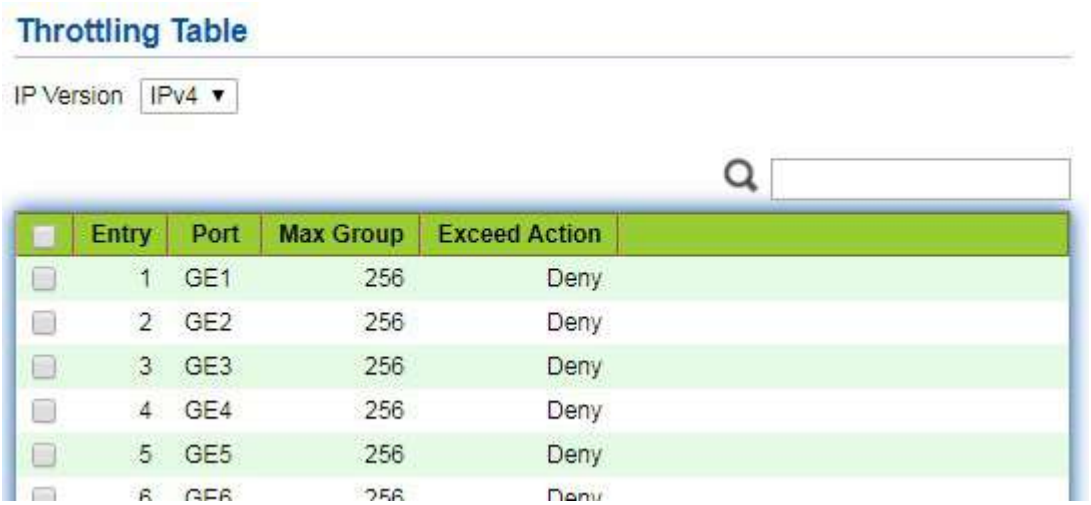
멀티캐스트 전달 포트 구성 및 보기

1. 다음과 같이 네비게이션 바에서 “Multicast > General > Forward All ”을 클릭하세요.

12.1.5 Throttling

포트 멀티캐스트 그룹 제한 구성 및 보기

1. 다음과 같이 네비게이션 바에서 “Multicast > General > Throttling”을 클릭하세요.



12.1.6 프로필 필터링

포트 멀티캐스트 필터링 프로필 구성 및 보기

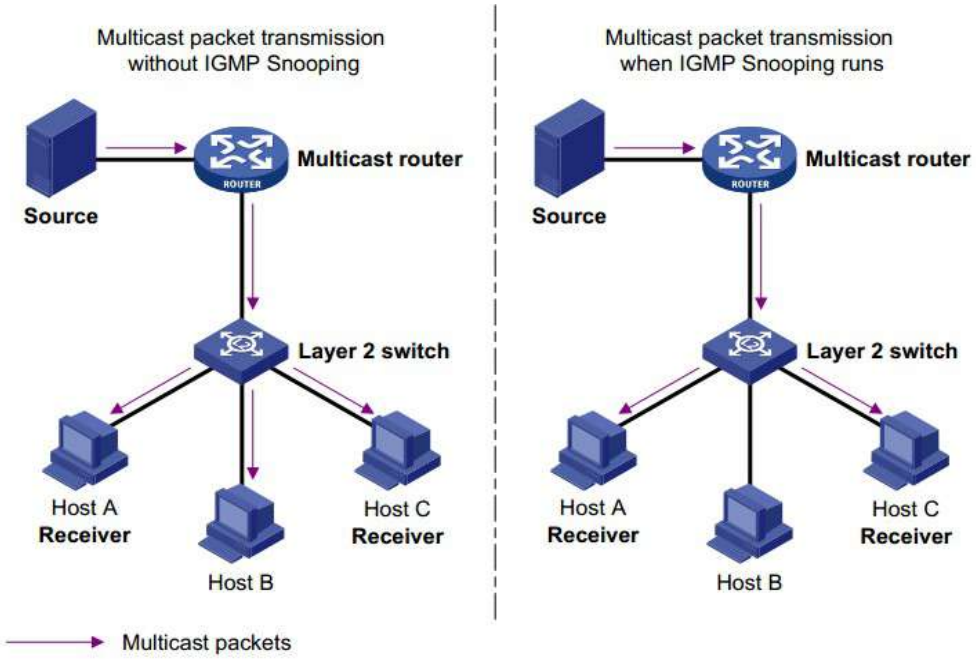
1. 다음과 같이 탐색 표시줄에서 “Multicast > General > Filtering Profile ”을 클릭합니다.

멀티캐스트 필터링 프로필 및 포트 바인딩 관계 구성 및 보기

2. 다음과 같이 네비게이션 바에서 “Multicast > General > Filtering Binding”을 클릭하세요.

12.2 IGMP 스누핑

IGMP 스누핑(인터넷 그룹 관리 프로토콜 스누핑)은 멀티캐스트 그룹을 관리하고 제어하기 위한 L2 장치의 제약 메커니즘입니다.
L2 장치는 수신된 IGMP 메시지를 분석하여 포트와 MAC 멀티캐스트 주소 간의 매핑을 설정하고 이에 따라 멀티캐스트 데이터를 전달합니다.
아래와 같이 멀티캐스트 데이터는 IGMP 스누핑 없이 L2 에서 전송됩니다. IGMP 스누핑이 실행되면 알려진 멀티캐스트 그룹 데이터는 지정된 수신자에게 전송되고 알려지지 않은 멀티캐스트 데이터는 여전히 계층 2 에 있습니다.

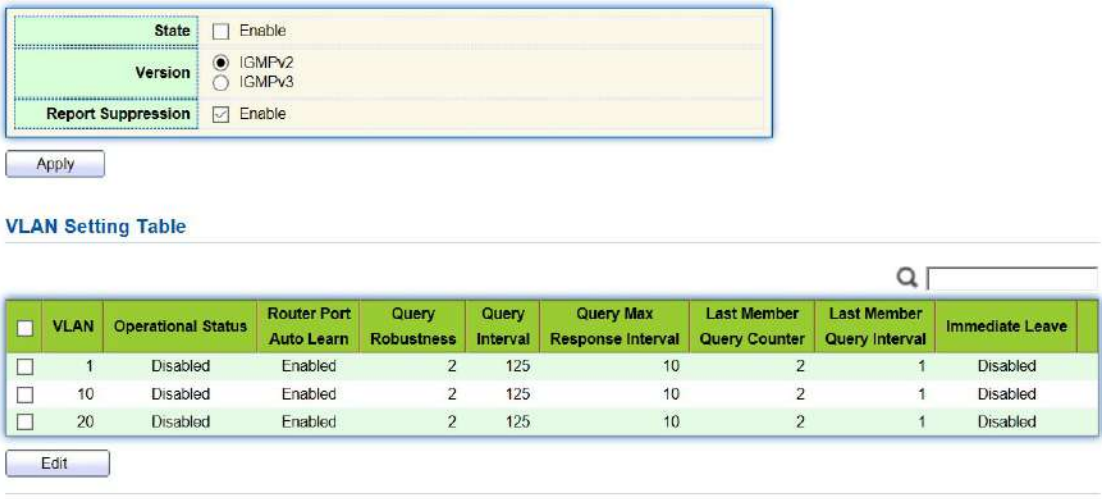


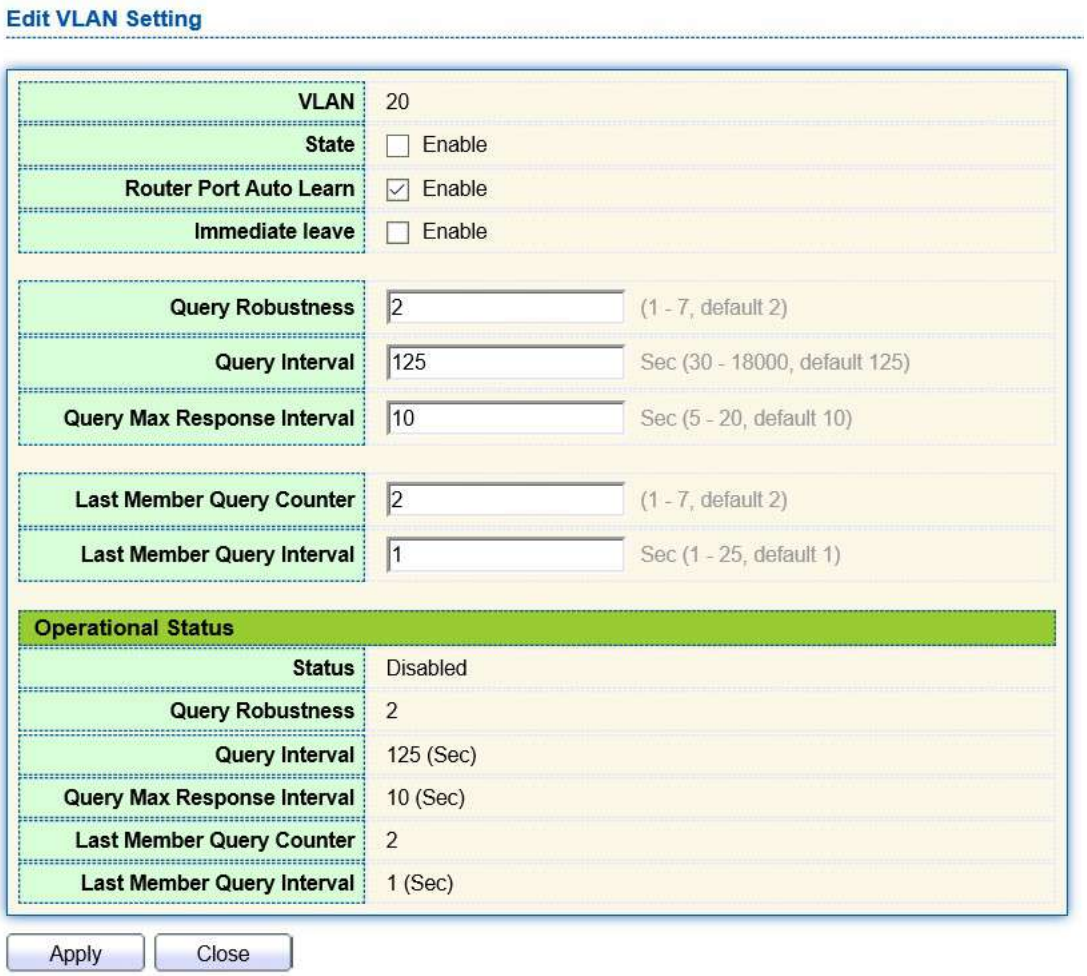
12.2.1 프로퍼티

IGMP 스누핑은 멀티캐스트 라우터와 사용자 호스트 사이의 L2 스위치에 있으며 IPv4 네트워크 배포에 적용 가능합니다. L2 네트워크에서 멀티캐스트 데이터 포워딩을 관리 및 제어하기 위해 라우터와 호스트 간에 전송되는 IGMP/MLD 메시지를 스누핑하고 멀티캐스트 데이터에 대한 L2 포워딩 테이블을 설정하도록 VLAN 에 구성됩니다.

글로벌 IGMP 스누핑 기능은 기본적으로 비활성화되어 있으므로 활성화해야 합니다.

1. Multicast > IGMP Snooping > Property"를 클릭하고 생성된 VLAN 정보에서 구성할 VLAN 을 선택한 후 다음과 같이 세부 사항을 "Edit"합니다.





인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	구성할 VLAN ID
State	이 VLAN 에서 IGMP 스누핑을 활성화 또는 비활성화합니다.
Router Port Auto Learn	경로 포트 자동 학습 활성화 또는 비활성화
Immediate leave	멀티캐스트 구성원이 빨리 떠남
Query Robustness	견고성 변수를 사용하면 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다.
Query Interval	메시지 쿼리 사이의 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	특정 그룹에 대한 메시지 쿼리 간격

2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

12.2.2 Querier

IGMP 스누핑 쿼리어 구성 및 보기

1. 다음과 같이 탐색 표시줄에서 "Multicast > IGMP Snooping > Querier"를 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	멀티캐스트 VLAN
State	IGMP 스누핑 쿼리어 활성화 또는 비활성화
Operational Status	IGMP 스누핑 쿼리어 실행 상태
Version	쿼리어용 버전
Querier Address	쿼리자를 위한 멀티캐스트 주소

12.2.3 통계

IGMP 스누핑 통계 구성 및 보기

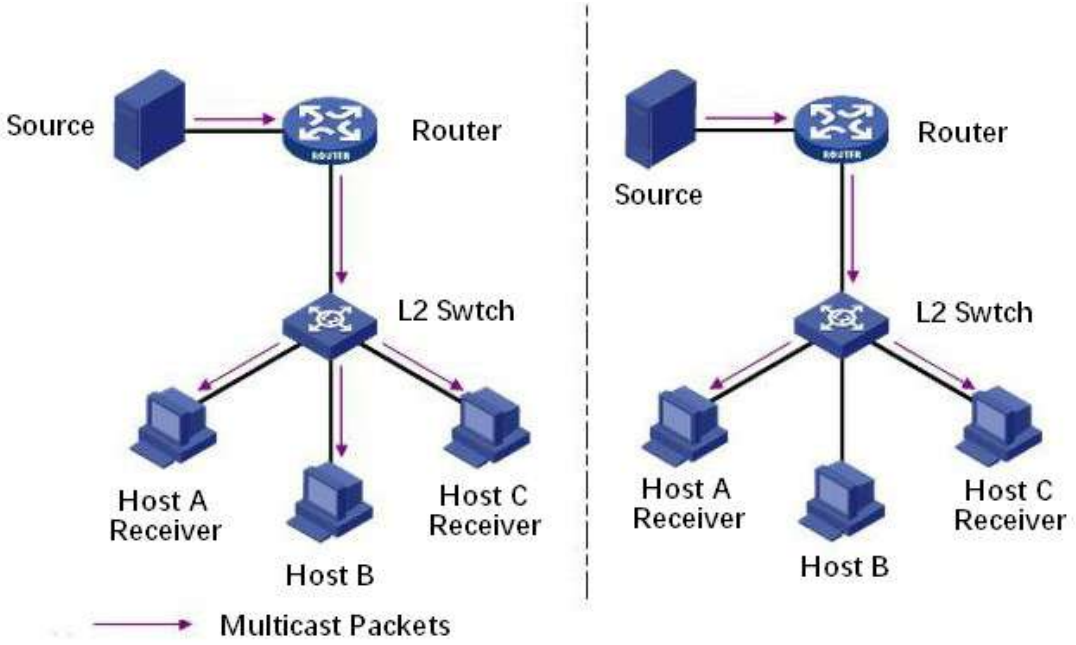
1. 다음과 같이 네비게이션 바에서 "Multicast > IGMP Snooping > Statistics"를 클릭하세요.

12.3 MLD 스누핑

MLD 스누핑은 멀티캐스트 Listener Discovery 스누핑의 약어입니다. 이는 IPv6 멀티캐스트 그룹을 관리하고 제어하는 데 사용되는 레이어 2 장치에서 실행되는 IPv6 멀티캐스트 제약 메커니즘입니다.

MLD 스누핑을 실행하는 두 번째 계층 장치는 수신된 MLD 메시지를 분석하여 포트와 MAC 멀티캐스트 주소 간의 매핑 관계를 설정하고 매핑 관계에 따라 IPv6 멀티캐스트 데이터를 전달합니다.

아래 그림에 표시된 것처럼 레이어 2 장치가 MLD 스누핑을 실행하지 않는 경우 IPv6 멀티캐스트 데이터 패킷은 레이어 2 에서 브로드캐스트됩니다. 레이어 2 장치가 MLD 스누핑을 실행할 때 알려진 IPv6 멀티캐스트 그룹의 멀티캐스트 데이터 패킷은 레이어 2 에서 브로드캐스트되지 않지만 레이어 2 의 지정된 수신기로 멀티캐스트됩니다.



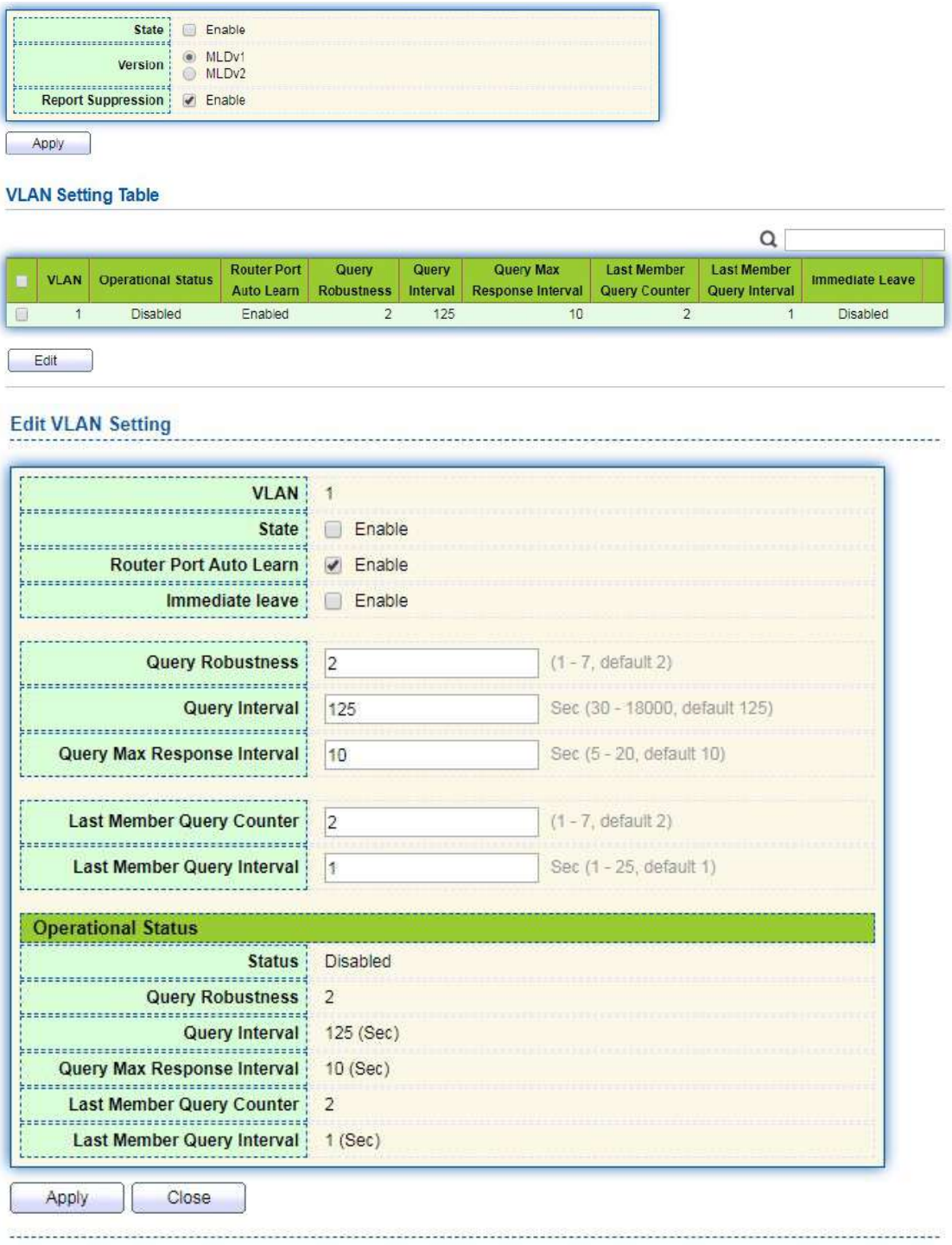
MLD 스누핑은 레이어 2 멀티캐스트를 통해 필요한 수신자에게만 정보를 전달할 수 있으며 이는 다음과 같은 이점을 가져올 수 있습니다.

- 레이어 2 네트워크의 브로드캐스트 패킷을 줄이고 네트워크 대역폭을 절약합니다.
- IPv6 멀티캐스트 정보의 보안을 강화합니다.
- 호스트별로 별도로 충전이 가능하여 편리합니다.

12.3.1 프로퍼티

로컬 MLD 스누핑 기능은 기본적으로 비활성화되어 있으므로 활성화해야 합니다.

1. “Multicast > MLD Snooping > Property”를 클릭하고 생성된 VLAN 정보에서 구성할 VLAN 을 선택한 후 다음과 같이 세부 사항을 “Edit”합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	구성할 VLAN ID
State	이 VLAN 에서 IGMP 스누핑을 활성화 또는 비활성화합니다.
Router Port Auto Learn	경로 포트 자동 학습 활성화 또는 비활성화

Immediate leave	멀티캐스트 구성원이 빨리 떠남
Query Robustness	견고성 변수를 사용하면 네트워크에서 예상되는 패킷 손실을 조정할 수 있습니다.
Query Interval	메시지 쿼리 사이의 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	특정 그룹에 대한 메시지 쿼리 간격

2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

12.3.2 통계

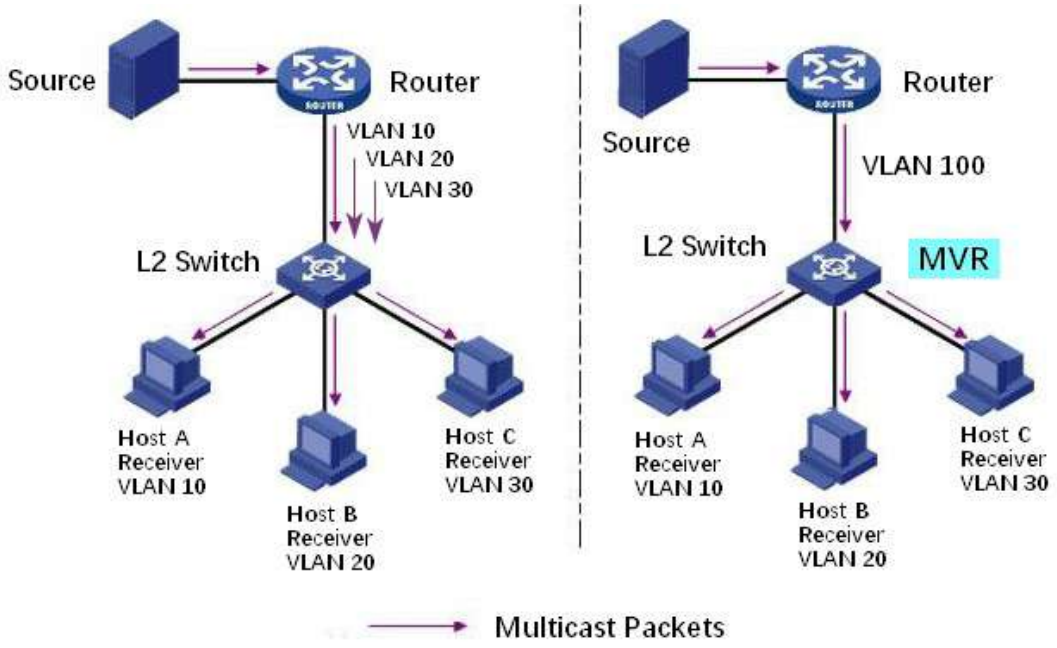
MLD 스누핑 통계 구성 및 보기

1. 다음과 같이 탐색 표시줄에서 "Multicast > MLD Snooping > statistics"를 클릭합니다.

12.4 MVR

레이어 2 네트워크에서 VLAN 기반의 멀티캐스트 트래픽 브로드캐스트 문제를 해결하기 위해 IGMP 스누핑 프로토콜을 사용하여 수신기를 제어합니다. 즉, 수신기만 멀티캐스트 트래픽을 정상적으로 수신할 수 있습니다.

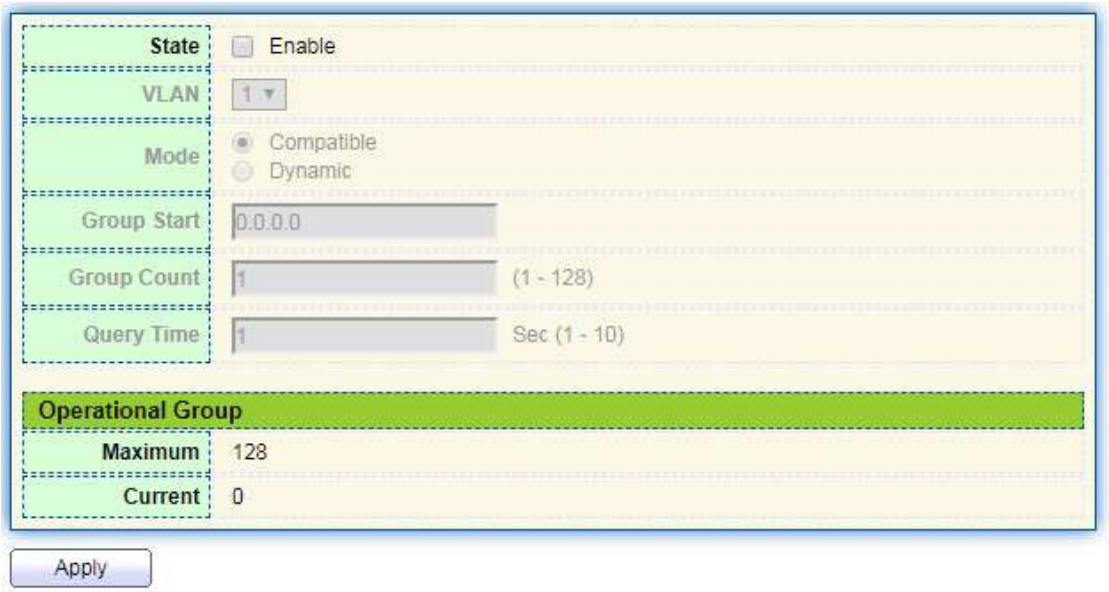
그러나 IGMP 스누핑은 동일한 멀티캐스트 VLAN 의 트래픽만 효과적으로 제어할 수 있으며 교차 VLAN 트래픽은 제어할 수 없습니다. 결과적으로 서로 다른 VLAN 에서 동일한 멀티캐스트를 여러 번 복제하는 효율성이 여전히 존재합니다. 크로스 VLAN 의 플러딩 문제를 해결하기 위해 아래 그림과 같이 멀티캐스트 소스 트래픽의 전용 멀티캐스트 VLAN 을 채택합니다.



12.4.1 프로퍼티

Global MVR 기능은 기본적으로 비활성화되어 있으므로 활성화해야 합니다.

1. “Multicast > MVR > Property”를 클릭하고 다음과 같이 MVR 글로벌 구성 인터페이스로 들어갑니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명

State	MVR 활성화 또는 비활성화
VLAN	구성할 VLAN ID
Mode	Compatible: MVR 스위치의 CPU 는 일반적으로 라우터의 쿼리 메시지와 클라이언트의 조인 메시지를 전달하여 동적 학습의 멀티캐스트 전달 테이블을 형성합니다. 그러나 CPU 는 Join 메시지를 라우터 포트로 전달하지 않으므로 상위 라우터는 다음 Join 메시지를 수신하지 못하므로 라우터 데이터가 스위치로 정상적으로 전달되지 않습니다. 이 모드에서는 라우터를 수동으로 구성해야 합니다. 멀티캐스트 포워딩 테이블은 데이터를 스위치로 전달합니다. Dynamic: 동적 모드와 호환 모드의 유일한 차이점은 CPU 가 동적 모드에서 조인 메시지를 라우터 포트로 전달할 수 있다는 것입니다. 따라서 상위 계층 라우터는 멀티캐스트 전달 테이블을 동적으로 학습할 수 있으며 수동으로 구성할 필요가 없습니다. 멀티캐스트 포워딩 테이블은 데이터를 스위치로 전달합니다.
Group Start	멀티캐스트 그룹의 시작 주소
Group Count	멀티캐스트 그룹 주소 수
Query Time	멀티캐스트 그룹 쿼리 시간

2. 해당 구성 항목을 입력합니다.
3. ""적용"하고 마무리합니다.

12.4.2 Port 설정

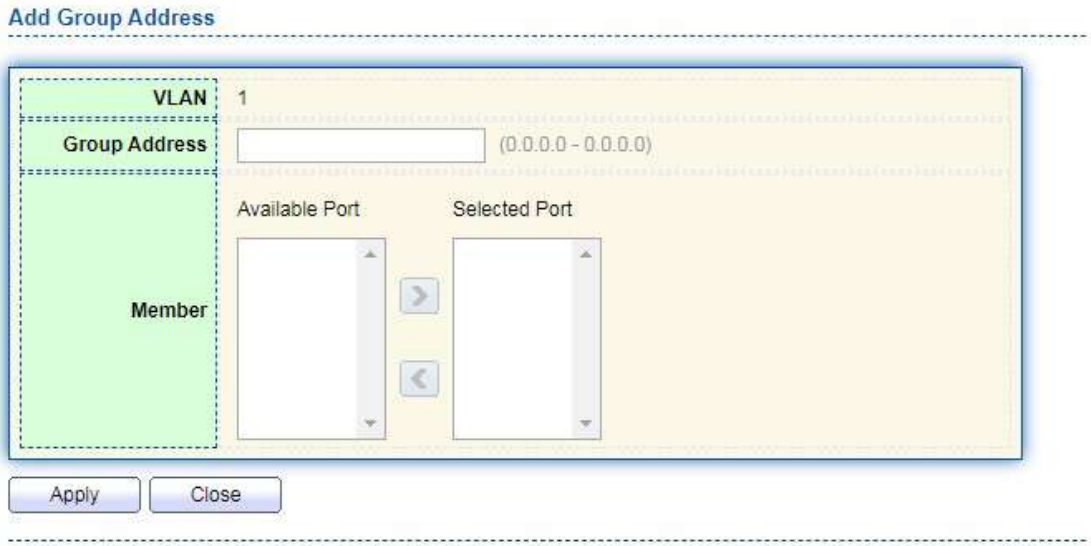
1. " Multicast > MVR > Port Setting "을 클릭하고 다음과 같이 MVR 포트 설정 인터페이스로 들어갑니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
Role	포트 모드 Receiver: 멀티캐스트 호스트가 연결된 스위치의 포트를 나타내며, 멀티캐스트 스트림을 수신하는 데 사용됩니다. Source: 소스 포트는 상위 계층 장비의 멀티캐스트 흐름의 소스 포트, 즉 멀티캐스트 소스 액세스 포트를 나타냅니다.
Immediate Leave	멀티캐스트 구성원은 빠르게 떠납니다.

12.4.3 그룹 주소

1. “Multicast > MVR > Group Address”를 클릭하면 다음과 같이 멀티캐스트 그룹 정보를 볼 수 있습니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	멀티캐스트용 VLAN ID
Group Address	멀티캐스트 주소를 입력하세요
Member	멀티캐스트 구성원 추가

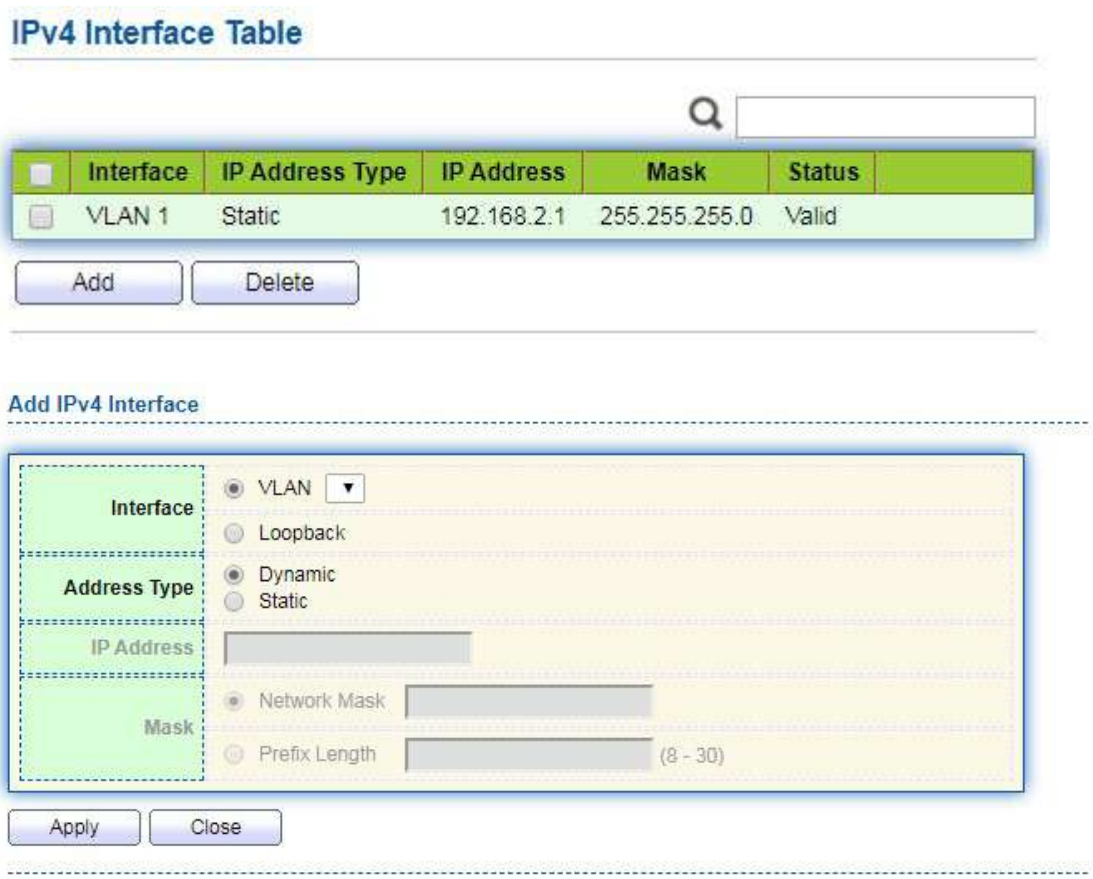
13 라우팅

스위치는 네트워크 계층 장치와 통신하는 데 사용되는 세 가지 VLAN 인터페이스 계층을 제공합니다. VLANIF 인터페이스는 IP 주소로 구성할 수 있는 네트워크 계층 인터페이스입니다. VLANIF 인터페이스를 생성하기 전에 해당 VLAN 을 먼저 생성해야 합니다. VLANIF 인터페이스의 도움으로 스위치는 다른 네트워크 계층 장치와 통신할 수 있습니다.

13.1 IPv4 관리 및 인터페이스

13.1.1 IPv4 인터페이스

1. " Routing > IPv4 Management and Interfaces > IPv4 Interface "를 클릭하고 다음과 같이 IPv4 레이어 3 인터페이스 구성을 입력합니다.

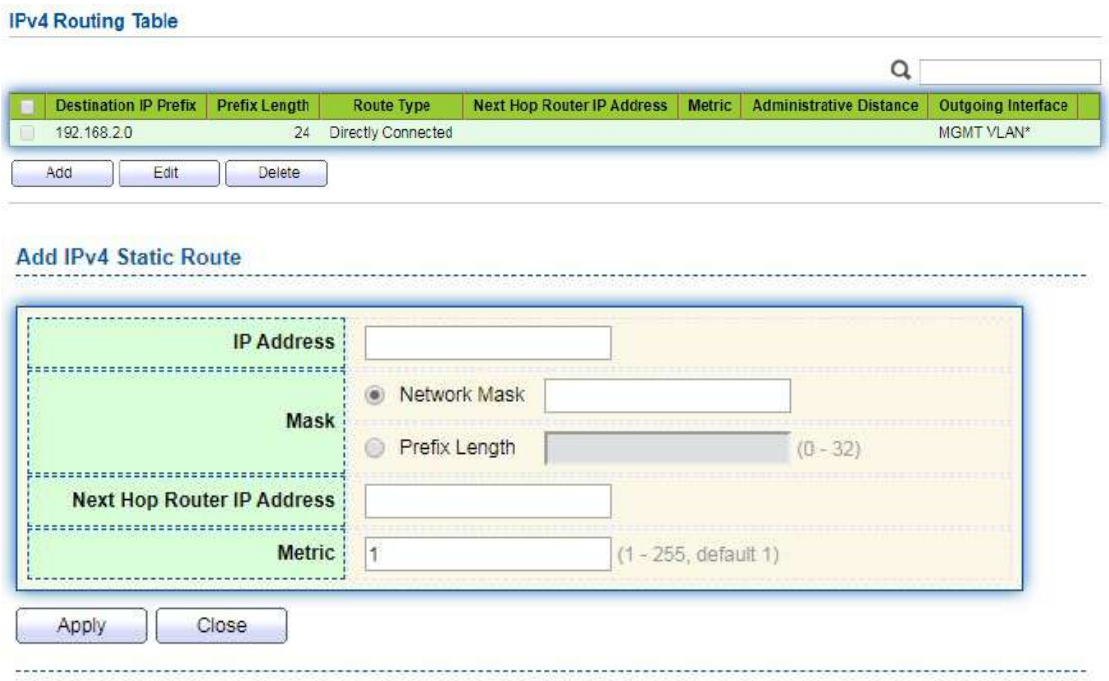


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	구성할 VLAN ID
Loopback	루프백 인터페이스
Address Type	Dynamic: 인터페이스의 IP 주소는 DHCP 에 의해 획득됩니다. Static: 인터페이스의 IP 주소는 수동으로 구성됩니다.
IP Address	인터페이스의 IP 주소
Mask	인터페이스의 IP 주소 마스크

13.1.2 IPv4 경로

1. " Routing > IPv4 Management and Interfaces > IPv4 Routes "를 클릭하고 다음과 같이 IPv4 고정 경로 인터페이스 구성을 입력합니다.

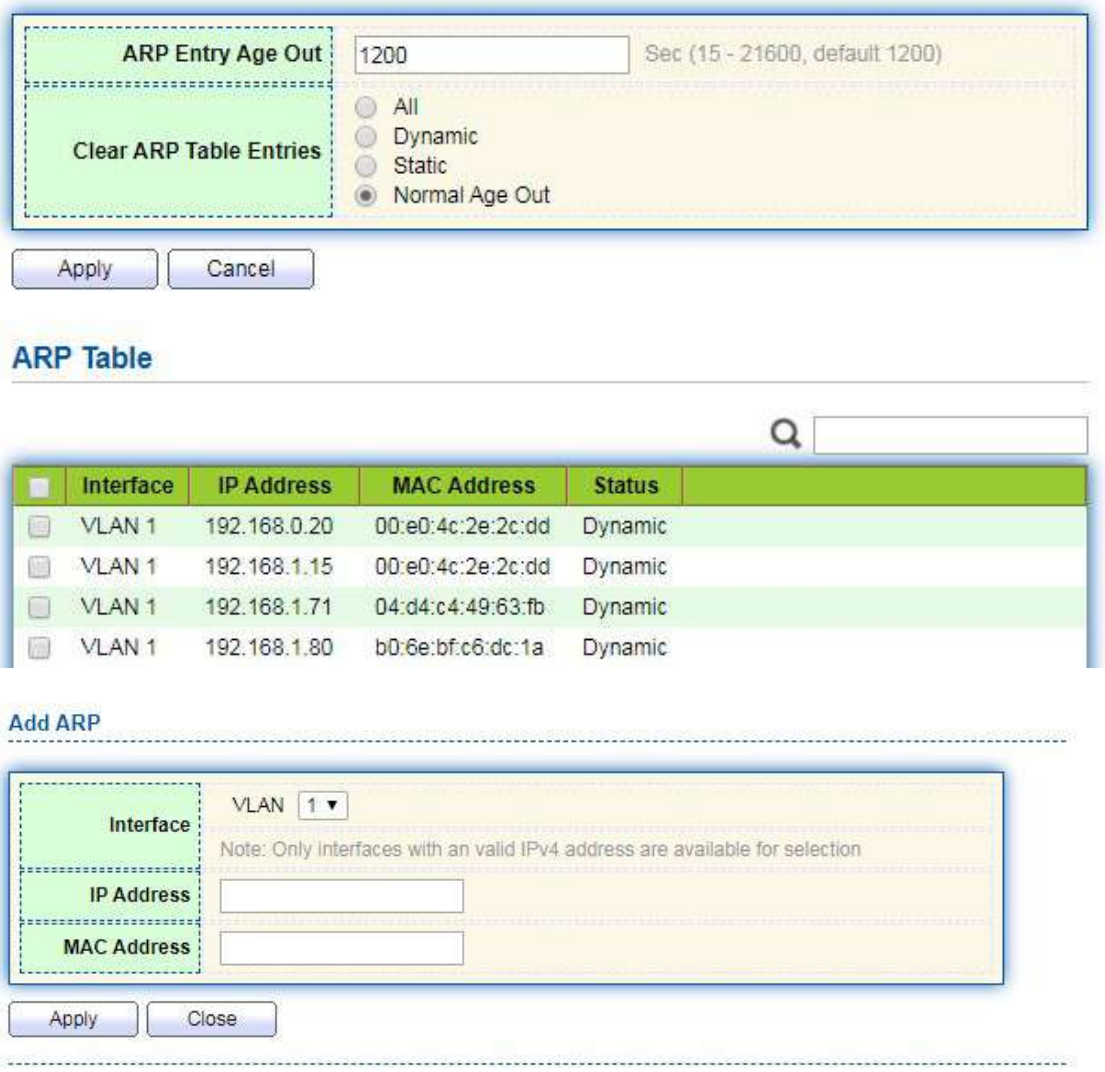


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
IP Address	대상 IP 주소 세그먼트
Mask	대상 IP 주소 마스크
Next Hop Router IP Address	다음 홉 IP 주소는 인터페이스 게이트웨이와 동일한 네트워크 세그먼트에 있어야 합니다.
Metric	네트워크 홉

13.1.3 ARP

1. " Routing > IPv4 Management and Interfaces >ARP "를 클릭하고 다음과 같이 ARP 테이블 항목을 구성하고 확인합니다.



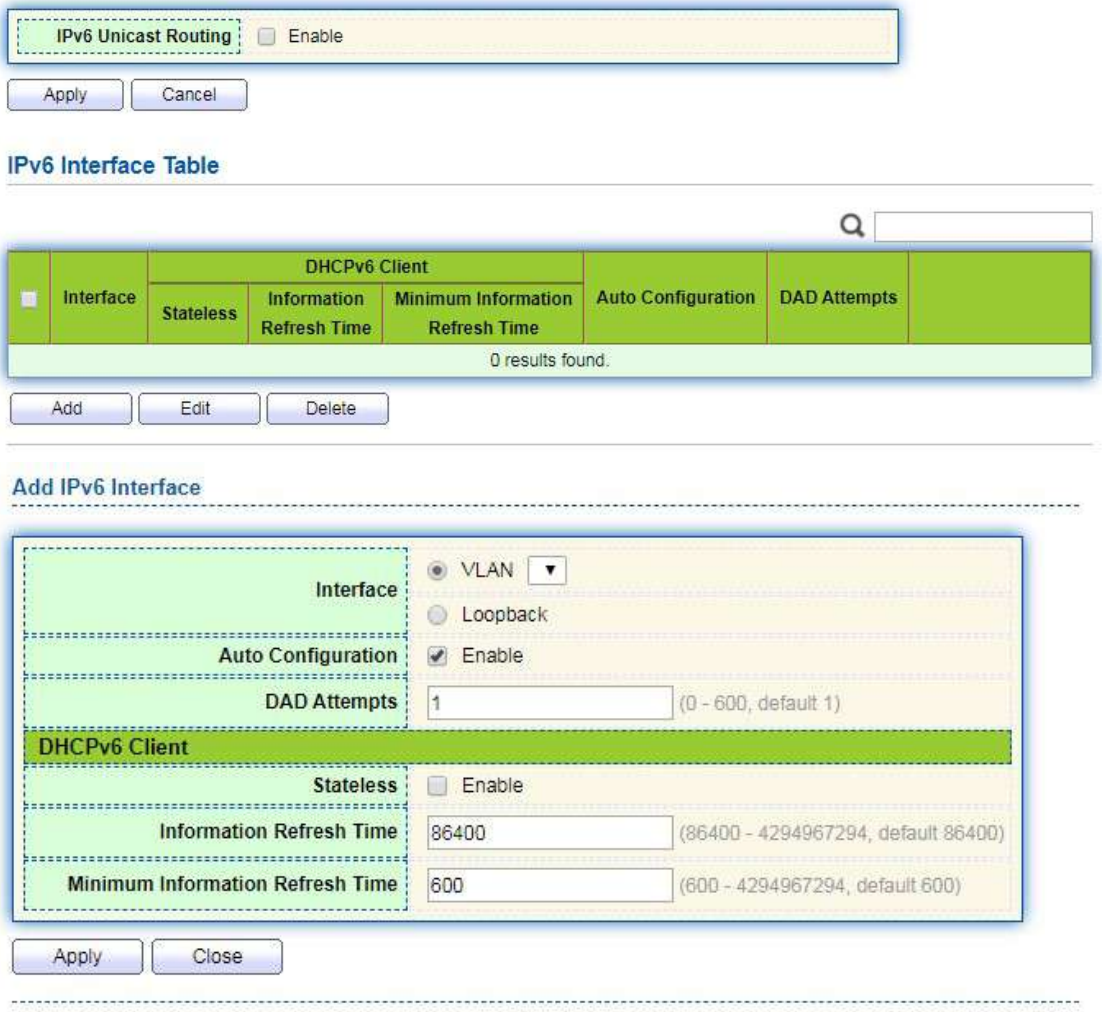
인터페이스 데이터는 다음과 같습니다.

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

13.2 IPv6 관리 및 인터페이스

13.2.1 IPv6 인터페이스

1. " Routing > IPv6 Management and Interfaces > IPv6 Interface "를 클릭하고 다음과 같이 IPv6 레이어 3 인터페이스 구성을 입력합니다.

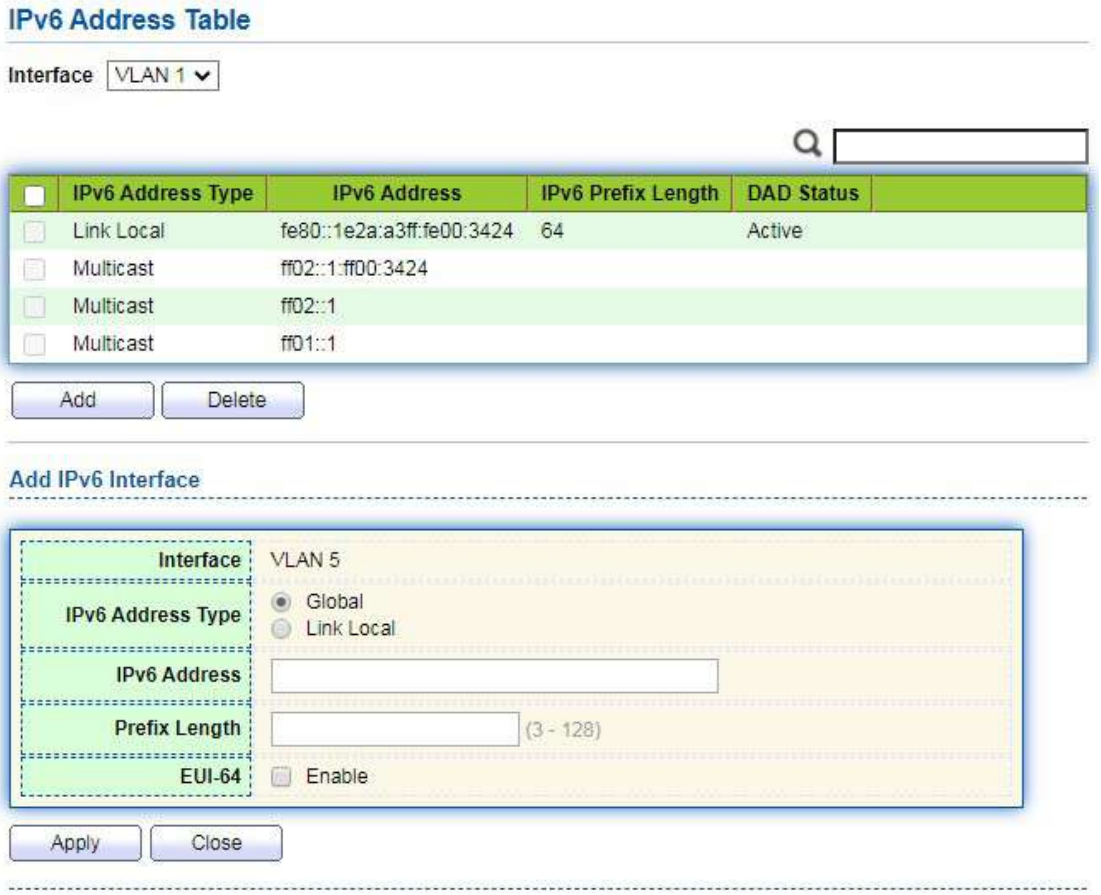


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
VLAN	구성할 VLAN ID
Loopback	루프백 인터페이스
Auto Configuration	자동 구성 스위치
DAD Attempts	중복 주소 감지를 위해 이웃 요청 메시지가 전송되는 횟수 구성
Stateless	상태 비저장 자동 구성
Information Refresh Time	자동 구성 새로 고침 시간
Minimum Information Refresh Time	자동 구성을 위한 최소 새로 고침 시간

13.2.2 IPv6 경로

1. " Routing > IPv6 Management and Interfaces > IPv6 Address "를 클릭하고 다음과 같이 IPv6 주소 구성 인터페이스를 입력합니다.

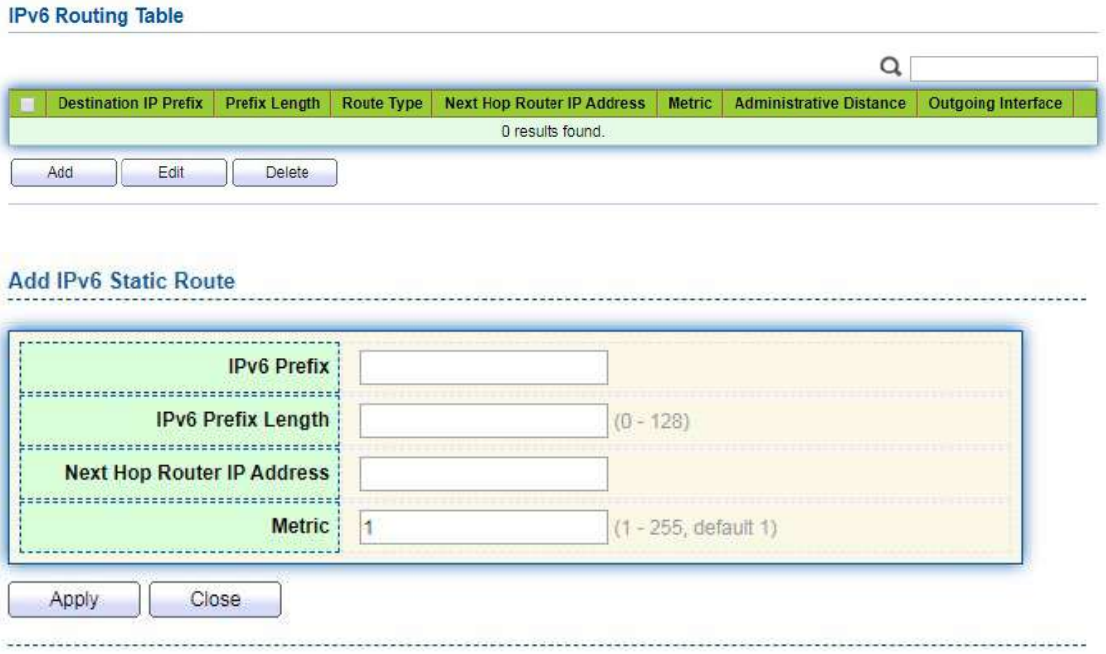


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Interface	VLANIF 인터페이스
IPv6 Address Type	Global: 글로벌 IPv6 주소 Link Local: 로컬 IPv6 주소
IPv6 Address	IPv6 주소
Prefix Length	IPv6 주소의 접두사
EUI-64	IEEE802 주소에서 파생된 주소를 활성화 또는 비활성화합니다.

13.2.3 IPv6 경로

1. " Routing > IPv6 Management and Interfaces > IPv6 Routes"를 클릭하고 다음과 같이 IPv6 고정 경로 인터페이스 구성을 입력합니다.

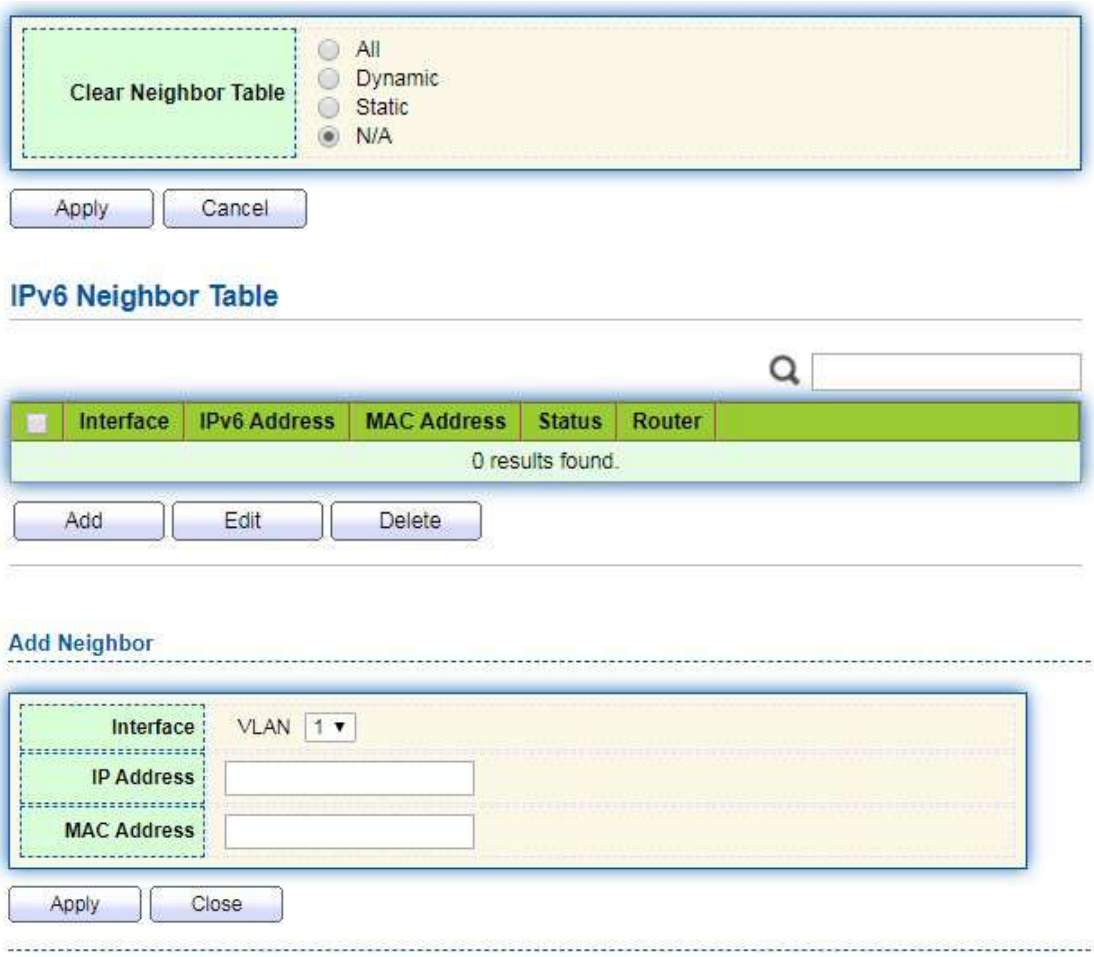


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
IPv6 Prefix	대상 IPv6 주소 세그먼트
IPv6 Prefix Length	대상 IPv6 주소 접두사
Next Hop Router IP Address	다음 홉 IPv6 주소는 인터페이스 게이트웨이와 동일한 네트워크 세그먼트에 있어야 합니다.
Metric	네트워크 홉

13.2.4 Neighbors

1. " Routing > IPv6 Management and Interfaces > Neighbors "를 클릭하고 다음과 같이 IPv6 인접 테이블 항목을 구성하고 확인합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Interface	VLANIF 인터페이스
IP Address	인터페이스 게이트웨이와 동일한 네트워크 세그먼트의 IPv6 주소
MAC Address	IPv6 주소에 해당하는 MAC 주소

13.3 Rip 경로 관리

RIP(라우팅 정보 프로토콜)는 상대적으로 오래되었지만 여전히 널리 사용되는 IGP(내부 게이트웨이 프로토콜)로 소규모 동종 네트워크에서 주로 사용됩니다. RIP 는 RFC 1058 에 등장하는 고전적인 거리 벡터 라우팅 프로토콜로, RFC1388 중에서 향상된 RIP-2 를 제시하고 RFC 1723 과 RFC 2453 에서 개정되었습니다.

RIP 는 Bellman-For 알고리즘을 사용하며 현재 RIP IPv4 에는 RIPv1 과 RIPv2 의 두 가지 버전이 있습니다. RIP 에는 다음과 같은 주요 기능이 있습니다. RIP 는 일반적인 거리 벡터 라우팅 프로토콜입니다.

브로드캐스트 주소 255.255.255.255 에서 보낸 RIP 메시지, RIPv2 는 UDP 의 포트 520 을 사용하여 멀티캐스트 주소 224.0.0.9 를 사용하여 메시지를 보냅니다.
RIP 는 링크의 대역폭과 지연이 아닌 라우팅 메트릭으로 대상 네트워크에 대한 최소 홉 수를 사용합니다.
RIP 는 소규모 네트워크용으로 설계되었습니다. 홉 수는 15 홉으로 제한되며, 16 홉에는 도달할 수 없습니다.
RIP-1 은 일종의 클래스 라우팅 프로토콜로, 불연속적인 서브넷 설계를 지원하지 않습니다.
RIP-2 는 CIDR 및 VLSM 가변 서브넷 마스크를 지원하여 불연속 서브넷 마스크 설계를 지원합니다.
RIP 주기적인 전체 라우팅 업데이트, 라우팅 테이블을 이웃 라우터로 브로드캐스트합니다. 브로드캐스트 주기는 기본적으로 30 초입니다.
RIP 프로토콜 관리 거리는 120 입니다.

소규모 네트워크의 경우 점유 대역폭 측면에서 RIP 는 비용이 저렴하고 구성, 관리 및 구현이 용이하며 RIP 가 여전히 사용되고 있습니다. 그러나 RIP 에는 분명한 단점도 있습니다. 네트워크가 두 개 이상일 경우 루프 문제가 나타납니다. 루프 문제를 해결하기 위해 IETF 는 분할-수평(split-Horizon) 방식을 제안했는데, 이 인터페이스에서 수신된 라우팅 정보는 더 이상 인터페이스 밖으로 나가지 않습니다. 분할 범위는 두 라우터 사이의 라우팅 루프 문제를 해결하지만 대규모 네트워크로 인해 주로 지연 요인에 의해 루프가 형성되는 문제를 방지할 수는 없습니다. 트리거 업데이트를 위해서는 링크가 변경될 때 라우터가 라우팅 테이블을 즉시 전송해야 합니다. 이를 통해 네트워크 수렴 속도가 빨라지지만 브로드캐스트 플러딩이 발생하기 쉽습니다. 즉, 루프 문제를 해결하려면 일정량의 시간과 대역폭을 소비해야 합니다. RIP 프로토콜을 채택하면 네트워크의 링크 수가 15 개를 초과할 수 없으므로 RIP 프로토콜은 대규모 네트워크에 적합하지 않습니다.

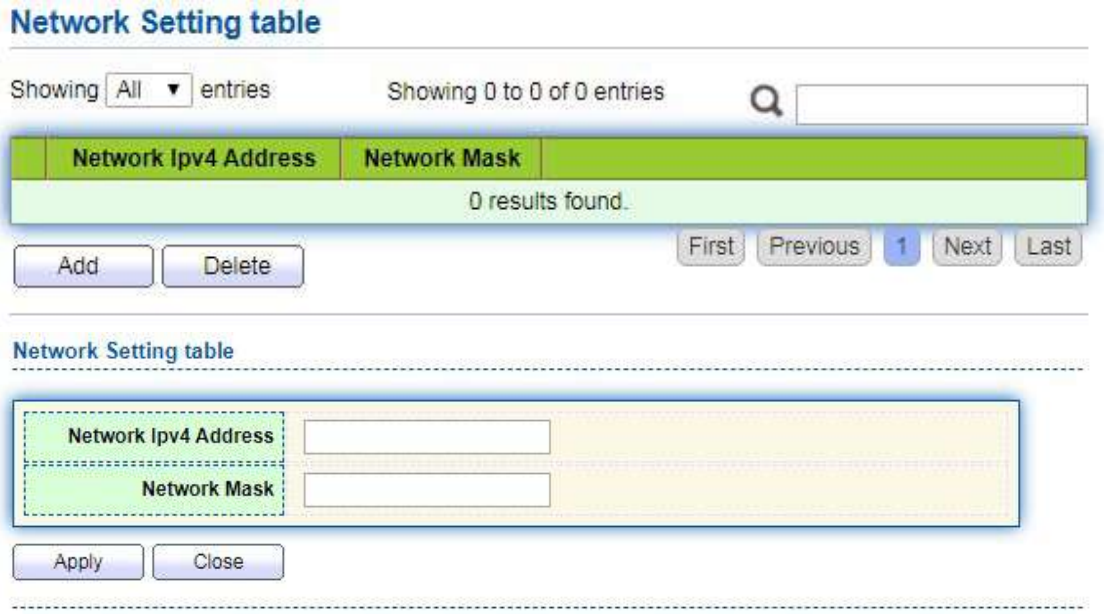
RIP 작동 원리

RIP 는 인터넷 표준 프로토콜인 거리 벡터(Distance Vector) 기반의 분산형 라우팅 프로토콜이다. 가장 큰 장점은 간단합니다. RIP 프로토콜에서는 네트워크의 각 라우터가 자신과 다른 대상 네트워크 사이의 거리 기록을 유지해야 합니다. RIP 프로토콜은 "거리"를 다음과 같이 정의합니다. 직접 연결된 네트워크의 라우터 거리는 1 로 정의됩니다. 직접 연결되지 않은 네트워크의 라우터 거리는 각 라우터에 1 을 더한 것으로 정의됩니다. "거리"는 "홉"이라고도 합니다. RIP 에서는 하나의 경로에 최대 15 개의 라우터가 포함될 수 있으므로 16 에 해당하는 거리에는 도달할 수 없습니다. 따라서 RIP 프로토콜은 소규모 인터넷에만 적용됩니다.
RIP 2 는 RIP 에서 파생되었으며 RIP 의 보충 프로토콜입니다. 주로 로드되는 유용한 정보의 수를 늘리고 보안 성능을 높이는 데 사용됩니다. RIPv1 및 RIPv2 는 UDP 기반 프로토콜입니다. RIP2 에서는 각 호스트 또는 라우터가 라우팅 선택 프로세스를 통해 UDP 포트 520 에서 패킷을 보내고 받습니다. RIP

프로토콜의 기본 라우팅 업데이트 기간은 30 초입니다.

1. 다음과 같이 네비게이션 트리에서 “Routing > Rip Routes Management > Rip Routes Setting”을 클릭합니다.

2. 네트워크 설정 테이블에서 "추가"를 클릭하면 다음과 같이 구성 인터페이스로 들어갑니다.



Notice:
네트워크를 구성하고 게시하기 전에 인터페이스 IP 를 구성하고 인터페이스의 IP 프로토콜과 물리적 상태가 작동하는지 확인하세요.

13.4 Ospf 경로 관리

OSPF(Open Shortest Path First)는 단일 자율 시스템(AS) 내에서 라우팅 결정을 위한 IGP(Interior Gateway Protocol)입니다. 내부 게이트웨이 프로토콜(IGP)에 따라 링크 상태 라우팅 프로토콜을 구현한 것입니다. 자율 시스템 내에서 작동됩니다. 최단 경로는 Dixdale 알고리즘을 사용하여 계산됩니다.

OSPF 는 IETF 의 OSPF 작업 그룹에서 개발한 IGP 라우팅 프로토콜입니다. IP 네트워크용으로 설계된 OSPF 는 IP 서브넷 및 외부 라우팅 정보 표시를 지원하며 메시지 인증도 허용하고 IP 멀티캐스트를 지원합니다.

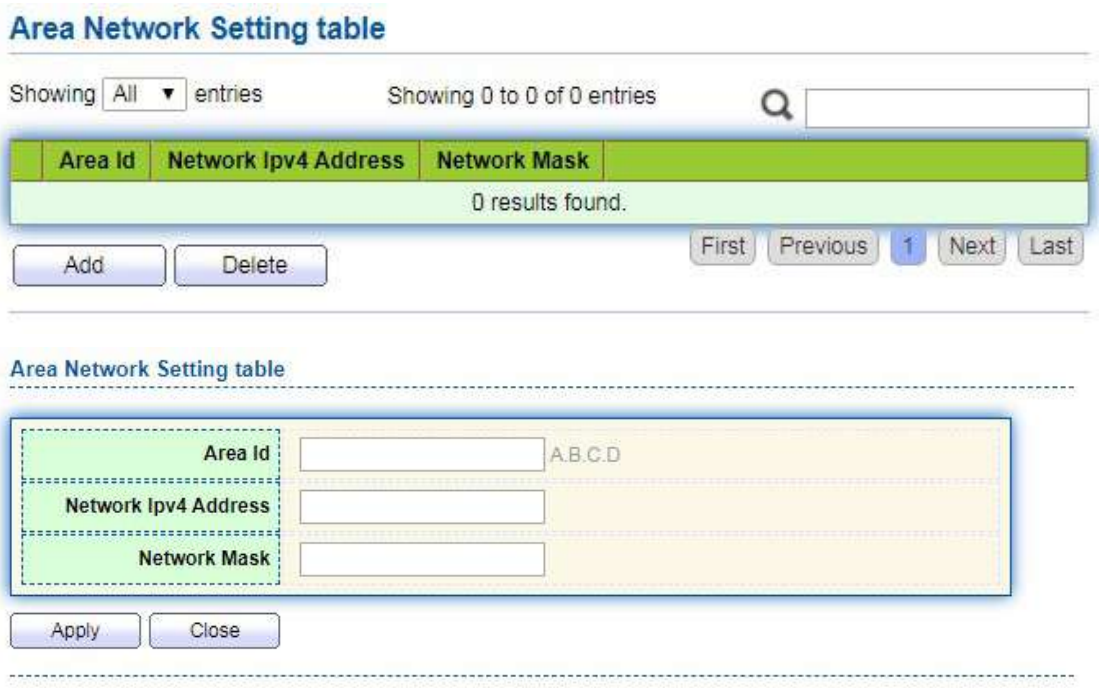
OSPF 라우팅 프로토콜은 일반적인 링크 상태 라우팅 프로토콜로, 일반적으로 동일한 라우팅 도메인에서 사용됩니다. 여기서 라우팅 도메인이란 통일된 라우팅 정책이나 라우팅 프로토콜을 통해 라우팅 정보를 교환하는 네트워크 그룹을 의미하는 자율 시스템(as)을 의미합니다. 이 as 에서 모든 OSPF 라우터는 라우팅 도메인에서 해당 링크의 상태 정보를 저장하는 as 구조를 설명하는 동일한 데이터베이스를 유지 관리합니다. OSPF 라우터는 이 데이터베이스를 통해 OSPF 라우팅 테이블을 계산합니다.

OSPF 는 링크 상태 라우팅 프로토콜로서 거리 벡터 라우팅 프로토콜과 달리 링크 상태 멀티캐스트 데이터 LSA(링크 상태 광고)를 특정 지역의 모든 라우터에 전송합니다. 라우터 실행 거리 벡터 라우팅 프로토콜은 라우팅 테이블의 일부 또는 전부를 인접 라우터에 전달합니다.

정보 교환의 보안과 관련하여 OSPF 는 필요한 경우 라우터 간의 모든 정보 교환을 인증할 수 있도록 규정하여 신뢰할 수 있는 라우터만이 라우팅 정보를 전송할 수 있도록 보장합니다. OSPF 는 다양한 인증 메커니즘을 지원하며 서로 다른 지역 간에 서로 다른 인증 메커니즘을 사용할 수 있도록 합니다. OSPF 는 하드웨어 브로드캐스트 기능을 최대한 활용하여 링크 상태 메시지를 전송하기 위해 브로드캐스트 네트워크(예: 이더넷)에서 링크 상태 알고리즘 적용을 최적화합니다. 일반적으로 링크 상태 알고리즘의 토폴로지에서 노드는 라우터를 나타냅니다. k 개의 라우터가 모두 이더넷에 연결되어 있고 링크 상태가 브로드캐스트되면 이 K 개의 라우터에 대한 패킷이 K 의 제곱에 도달합니다. 따라서 OSPF 를 사용하면 노드가 토폴로지 다이어그램에서 브로드캐스트 네트워크를 나타낼 수 있습니다. 각 브로드캐스트 네트워크의 모든 라우터는 링크 상태 메시지를 보내 네트워크에 있는 라우터의 링크 상태를 보고합니다.

1. 다음과 같이 네비게이션 트리에서 “Routing > Ospf Routes Management > Ospf Routes Setting”을 클릭합니다.

2. 영역 네트워크 설정에서 "추가"를 클릭하면 다음과 같이 구성 인터페이스로 들어갑니다.

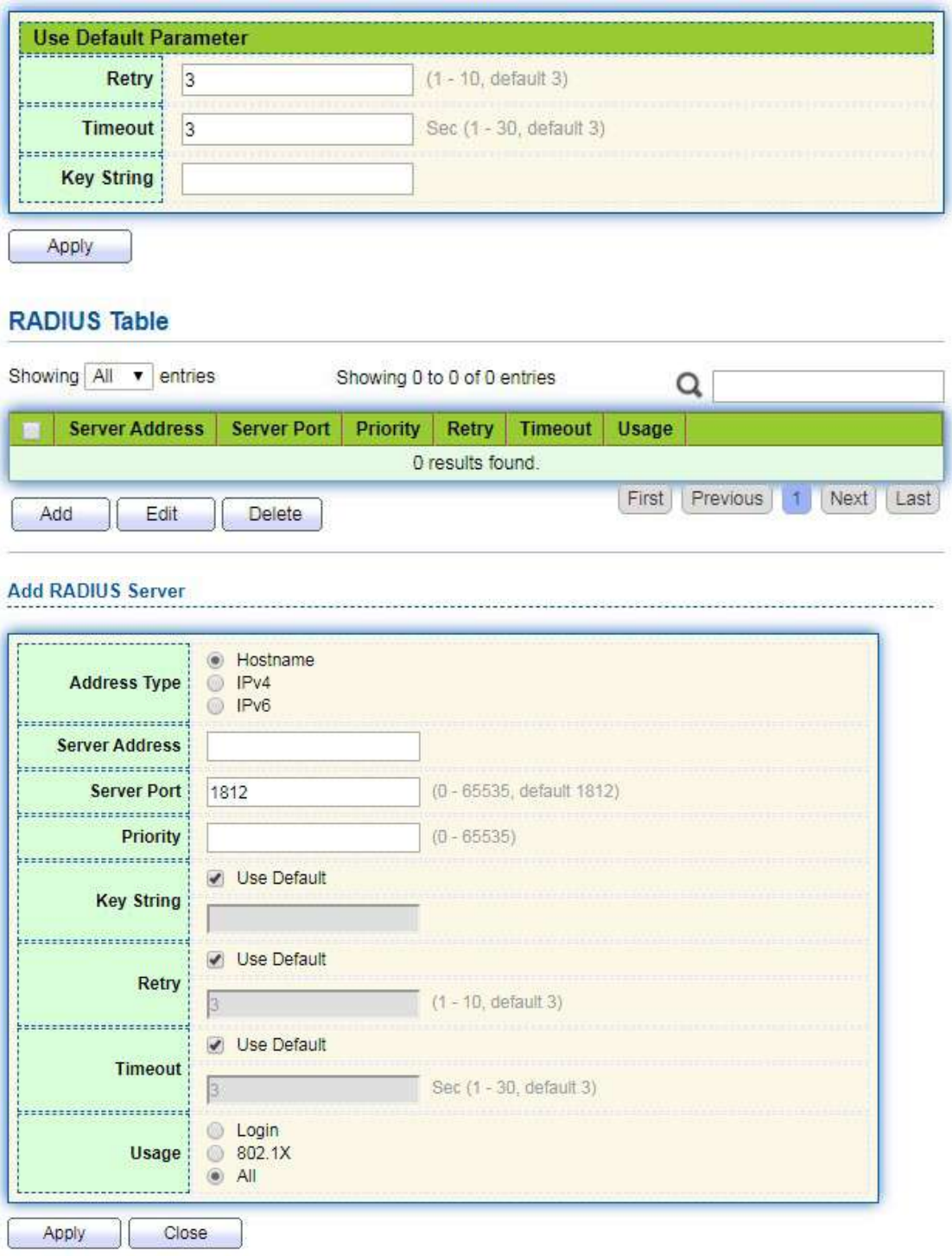


Notice:
네트워크를 구성하고 게시하기 전에 인터페이스 IP 를 구성하고 인터페이스의 IP 프로토콜과 물리적 상태가 작동하는지 확인하세요.

14 보안

14.1 RADIUS

1. " Security > RADIUS "를 클릭하고 다음과 같이 RADIUS 인터페이스로 들어갑니다.



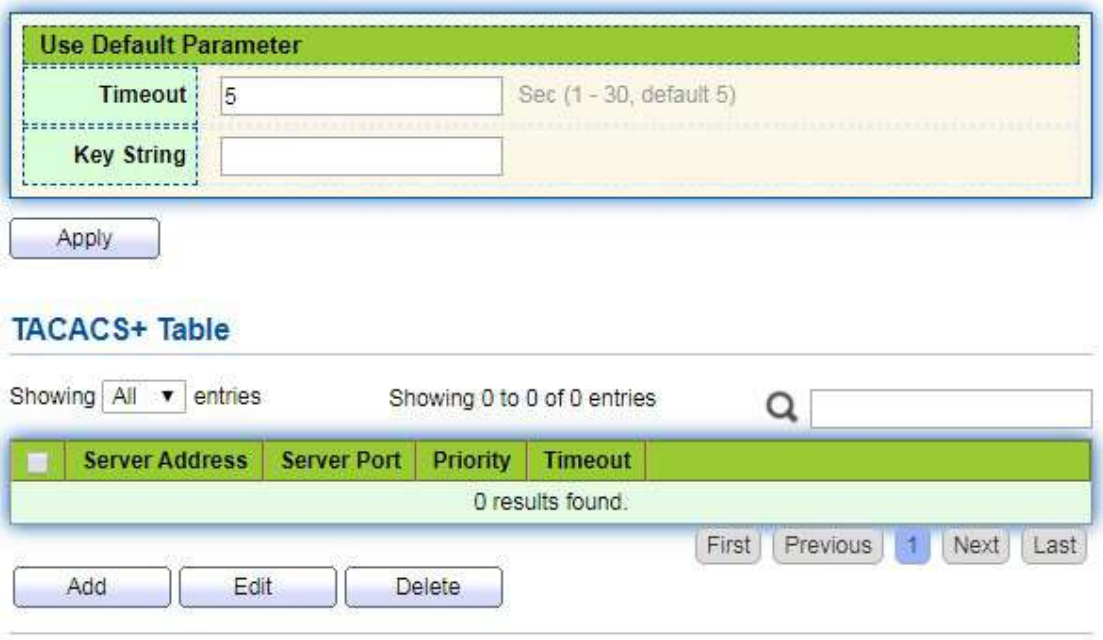
인터페이스 데이터는 다음과 같습니다.

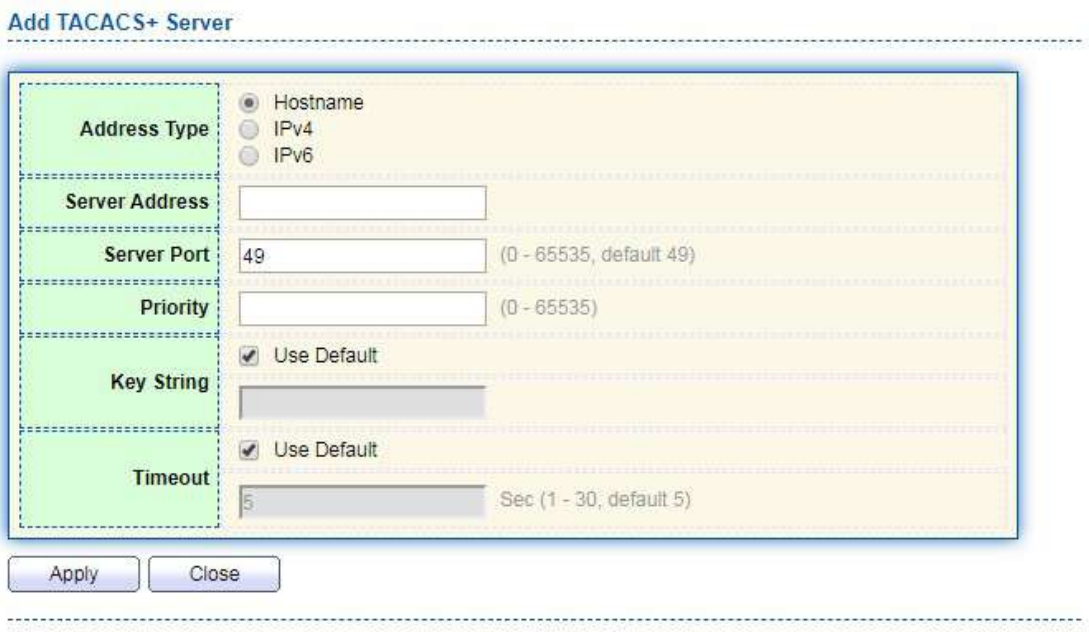
설정 항목	설명
Address Type	유형에 따라 호스트 이름, IPv4, IPv6 를 선택할 수 있습니다.
Server Address	서버의 IP 주소
Server Port	서비스 포트

Priority	서비스 우선순위
Key String	RADIUS 서버와 스위치 간에 공유되는 비밀 키
Retry	재전송 횟수는 횟수입니다.
Timeout	요청을 다시 전송하기 전에 RADIUS 서버의 응답을 기다립니다.
Usage	사용 시나리오

14.2 TACACS+

1. " Security > TACACS+"를 클릭하고 다음과 같이 TACACS+ 인터페이스로 들어갑니다.





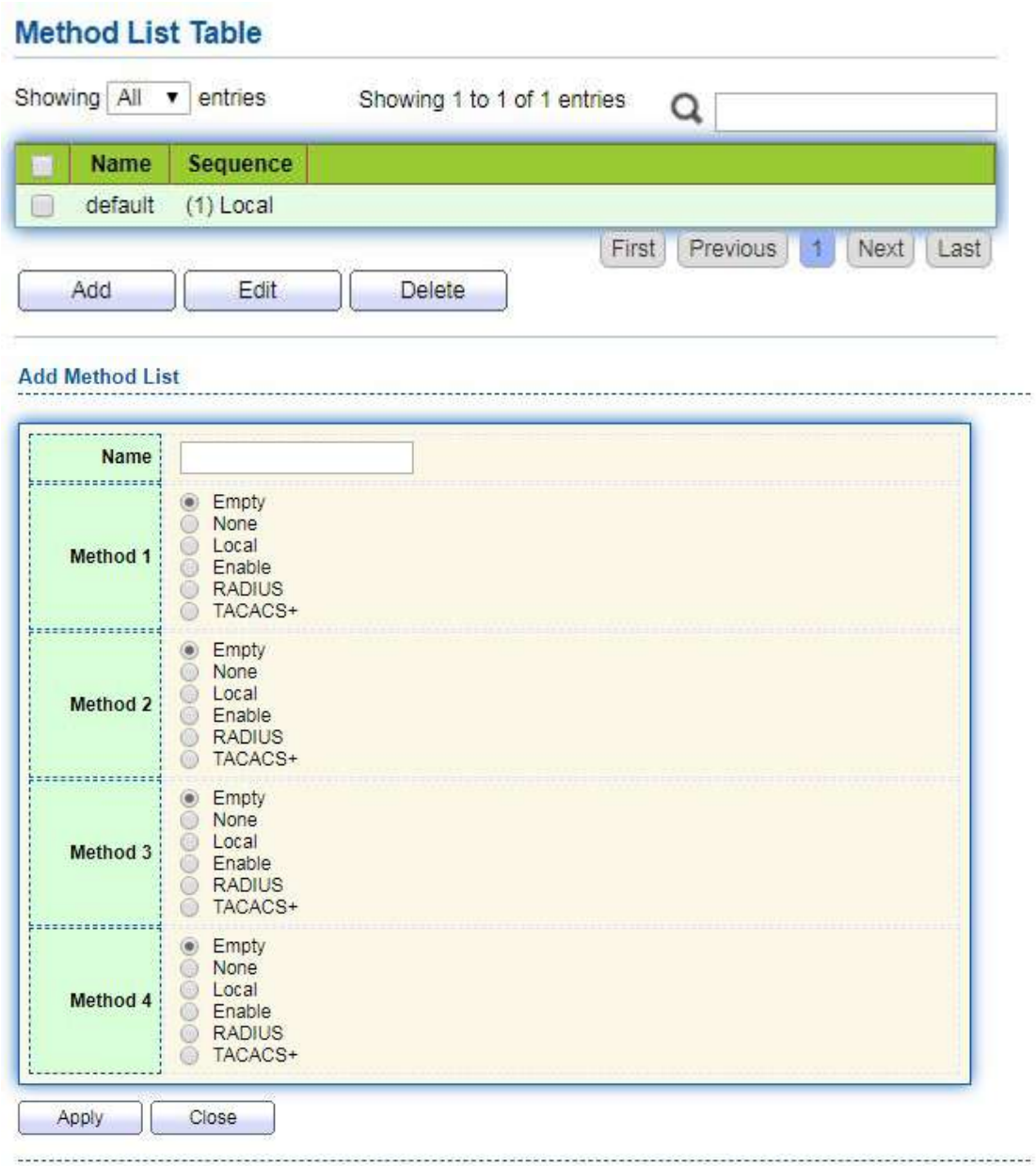
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Address Type	유형에 따라 호스트 이름, IPv4, IPv6 를 선택할 수 있습니다.
Server Address	서버의 IP 주소
Server Port	서비스 포트
Priority	서비스 우선순위
Key String	RADIUS 서버와 스위치 간에 공유되는 비밀 키
Retry	재전송 횟수는 횟수입니다.
Timeout	요청을 다시 전송하기 전에 RADIUS 서버의 응답을 기다립니다.

14.3 AAA

14.3.1 메소드 목록

1. " Security > AAA > Method List "을 클릭하고 다음과 같이 방법 목록 인터페이스로 들어갑니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Name	메소드 이름
Method 1-4	Empty: 방법이 비활성화되었습니다. None: 아무것도 하지 않고 사용자를 인증받도록 하세요. Local: 로컬 사용자 계정 데이터베이스를 사용하여 인증 Enable: 로컬 활성화 비밀번호 데이터베이스를 사용하여 인증 RADIUS: 원격 Radius 서버를 사용하여 인증 TACACS+: 원격 TACACS+ 서버를 사용하여 인증

14.3.2 로그인 인증

1. " Security > AAA > Login Authentication "을 클릭하고 다음과 같이 로그인 인증 인터페이스로 들어갑니다.

14.4 관리 액세스

14.4.1 관리 서비스

1. “Security > Management Access > Management Service”를 클릭하고 다음과 같이 관리 서비스 인터페이스로 들어갑니다.

2. “Security > Management Access > Management Service”를 클릭하고 다음과

같이 관리 서비스 인터페이스로 들어갑니다.

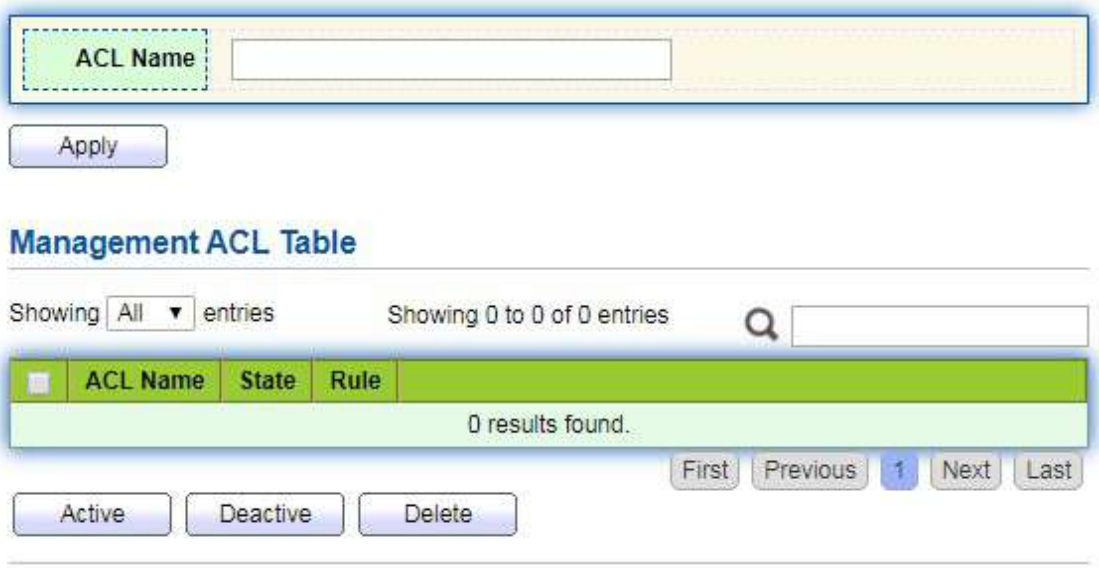
3. “Security > Management Access > Management Service”를 클릭하고 다음과 같이 관리 서비스 인터페이스로 들어갑니다.

4. “Security > Management Access > Management Service”를 클릭하고 다음과 같이 관리 서비스 인터페이스로 들어갑니다.

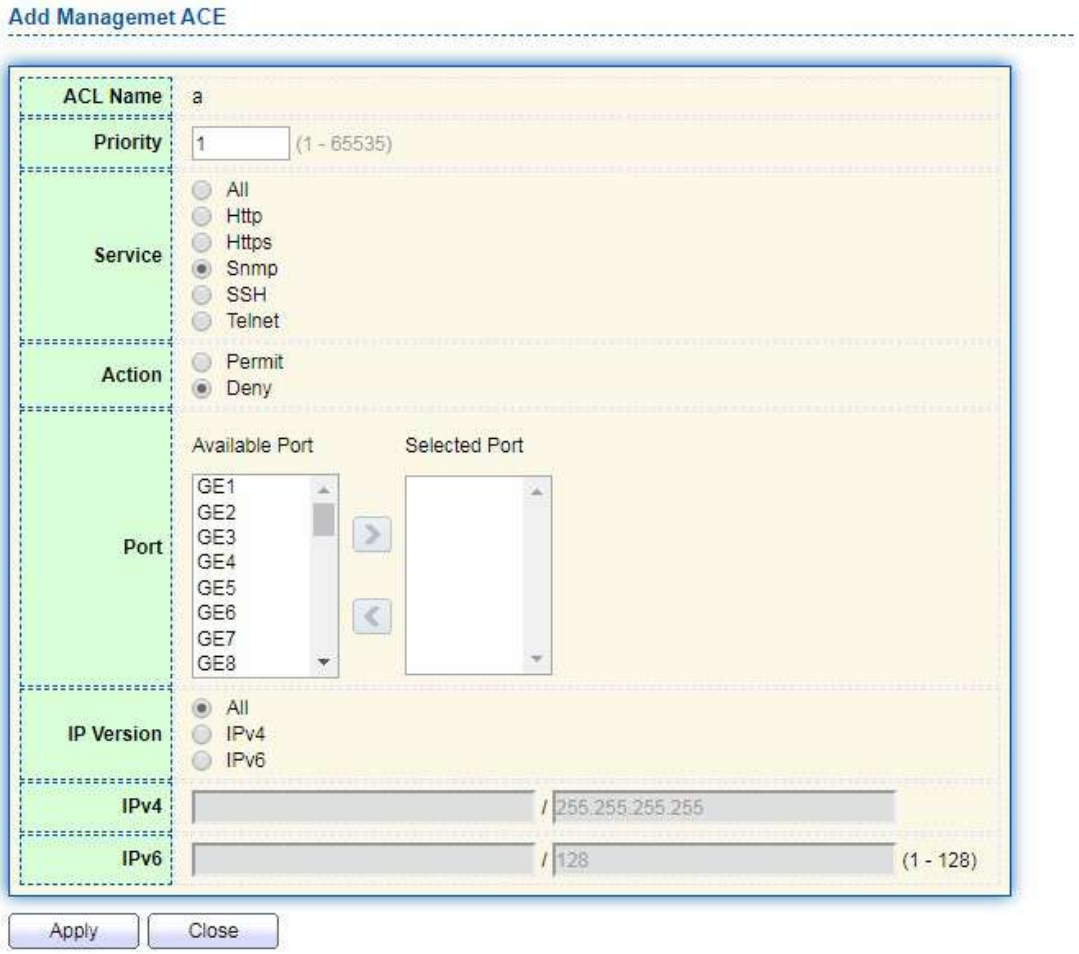
14.4.2 관리 ACL

ACLS 가 관리에 적용됨

1. " Security > Management Access > Management ACL "을 클릭하고 다음과 같이 관리 ALC 인터페이스로 들어갑니다.



2. " Security > Management Access > Management ACE "를 클릭하고 다음과 같이 관리 ACE 인터페이스로 들어갑니다.



인터페이스 데이터는 다음과 같습니다.

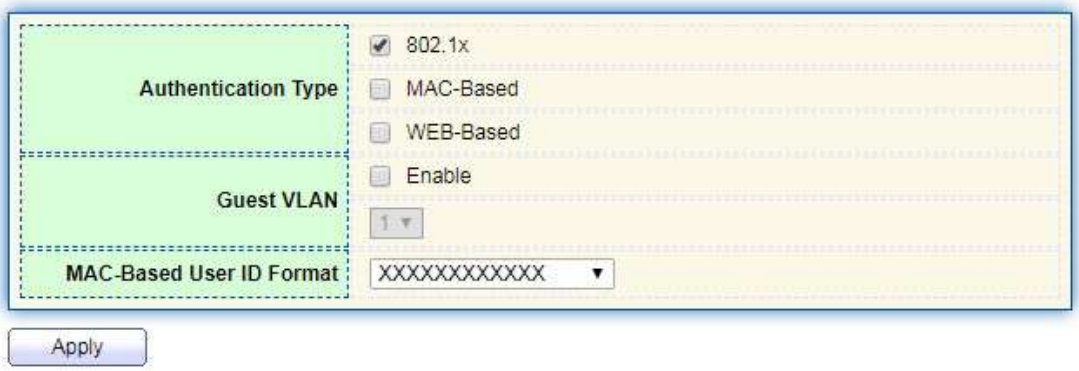
설정 항목	설명
ACL Name	ACL 이름
Priority	ACL 우선순위
Service	사용되는 서비스 유형
Action	매치 액션
Port	이 ACL 이 적용되는 포트
IP Version	IP 주소 버전 관리
IPv4	IPv4 주소
IPv6	IPv6 주소

14.5 인증 관리자

14.5.1 프로퍼티

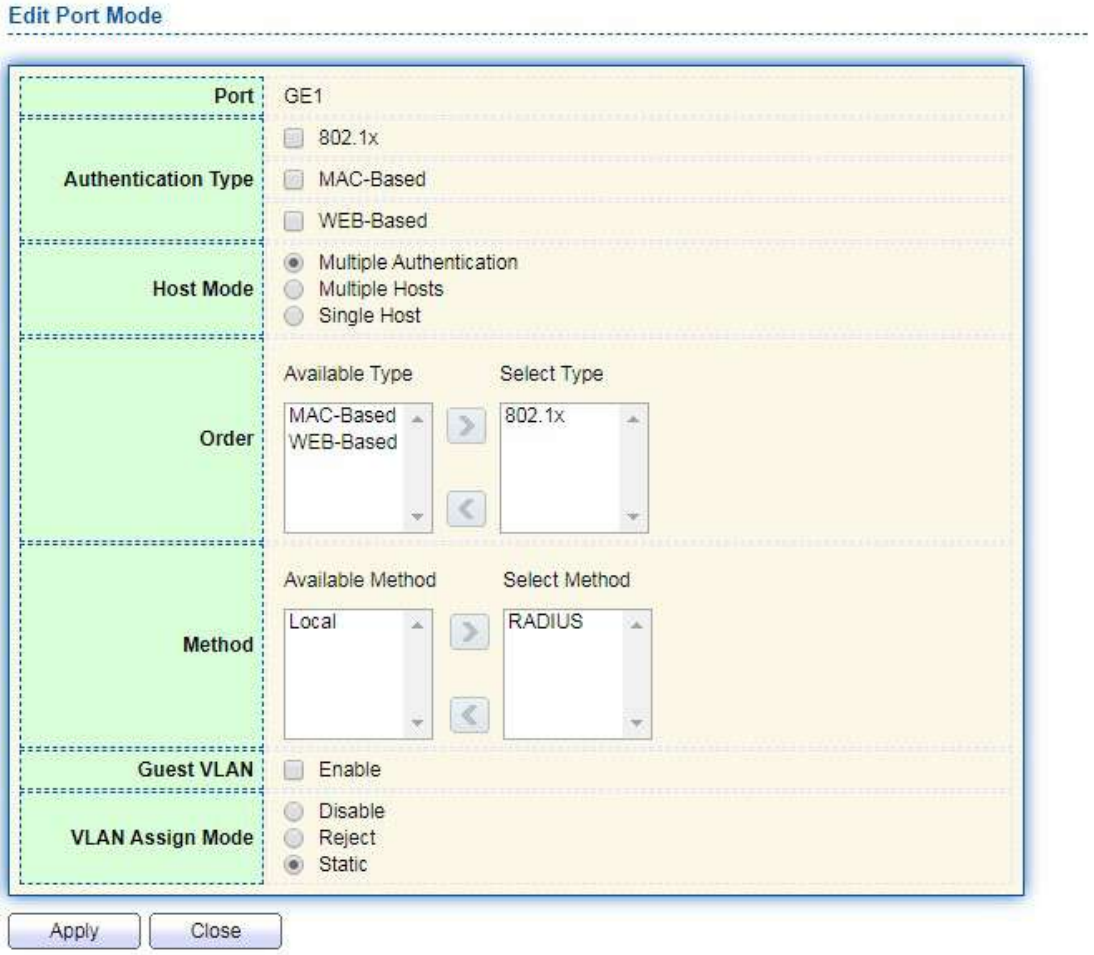
802.1x/MAC/WEB 인증 네트워크 접근 제어의 전역 설정을 활성화합니다.

1. “Security > Management Manager > Property”를 클릭하고 다음과 같이 글로벌 인터페이스로 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



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
Authentication Type	포트 인증 유형
Host Mode	Multiple Authentication: 이 모드에서는 모든 클라이언트가 개별적으로 인증 절차를 통과해야 합니다. Multiple Hosts: 이 모드에서는 하나의 클라이언트만 인증하면 되며 다른 클라이언트는 동일한 액세스 접근성을 갖게 됩니다. Single Host: 이 모드에서는 하나의 호스트만 인증될 수 있습니다. 최대 호스트 수를 1 로 구성하는 다중 인증 모드와 동일합니다.
Order	매치 액션
Method	포트 인증 방법 순서
Guest VLAN	게스트 VLAN

VLAN Assign Mode	포트 RADIUS VLAN 할당 모드 Reject: VLAN 인증 정보를 얻으면 이를 사용하십시오. 그러나 VLAN 인증 정보가 없으면 해당 호스트를 거부하고 인증되지 않은 상태로 만듭니다. Static: VLAN 인증 정보를 얻으면 이를 사용하십시오. VLAN 인증 정보가 없는 경우 호스트의 원래 VLAN 을 유지합니다.

14.5.2 포트 설정

1. " Security > Management Manager > Port Setting "을 클릭하고 다음과 같이 포트 설정 인터페이스로 들어갑니다.

Port Setting Table

Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

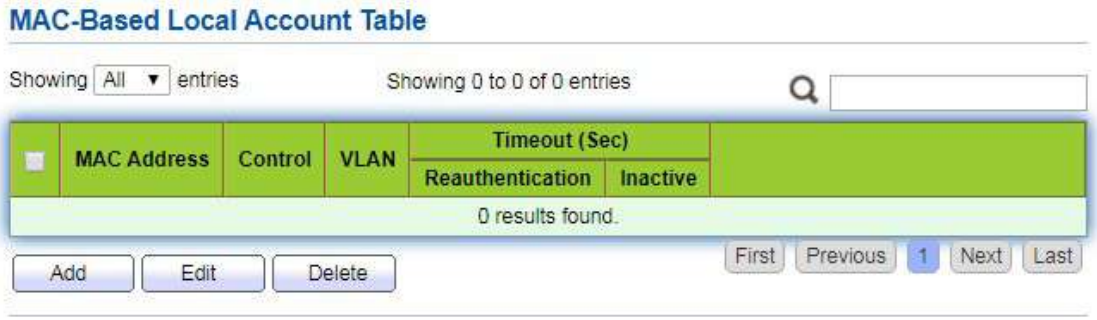
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
Port Control	Force Authorized: 포트가 강제로 승인되고 모든 클라이언트가 네트워크에 액세스할 수 있습니다. Force Unauthorized: 포트는 강제로 승인되지 않았으며 모든 클라이언트 Auto: 네트워크 접근성을 얻으려면 인증 절차 통과 필요
Reauthentication	포트 재인증 활성화
Max Hosts	다중 인증 모드의 포트 최대 호스트 수
Reauthentication	로컬 데이터베이스나 원격 인증 서버에서 재인증 시간을 할당하지 않은 경우 포트 재인증 기간 값(단위: 초)
Inactive	포트 비활성 시간 초과 값
Quiet	포트 휴면 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 WEB 인증 최대 로그인 시도 횟수

14.5.3 MAC 기반 로컬 계정

1. " Security > Management Manager > MAC-Based Local Account "을 클릭하고 다음과 같이 구성 인터페이스로 들어갑니다.

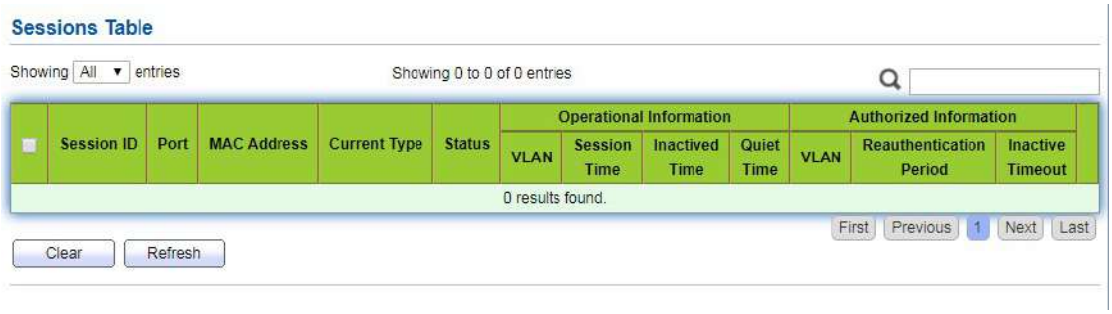


14.5.4 웹 기반 로컬 계정

1. “Security > Management Manager > WEB-Based Local Account”을 클릭하고 다음과 같이 구성 인터페이스로 들어갑니다.:

14.5.5 세션

1. " Security > Management Manager > Sessions "을 클릭하고 다음과 같이 세션 인터페이스를 확인하세요.

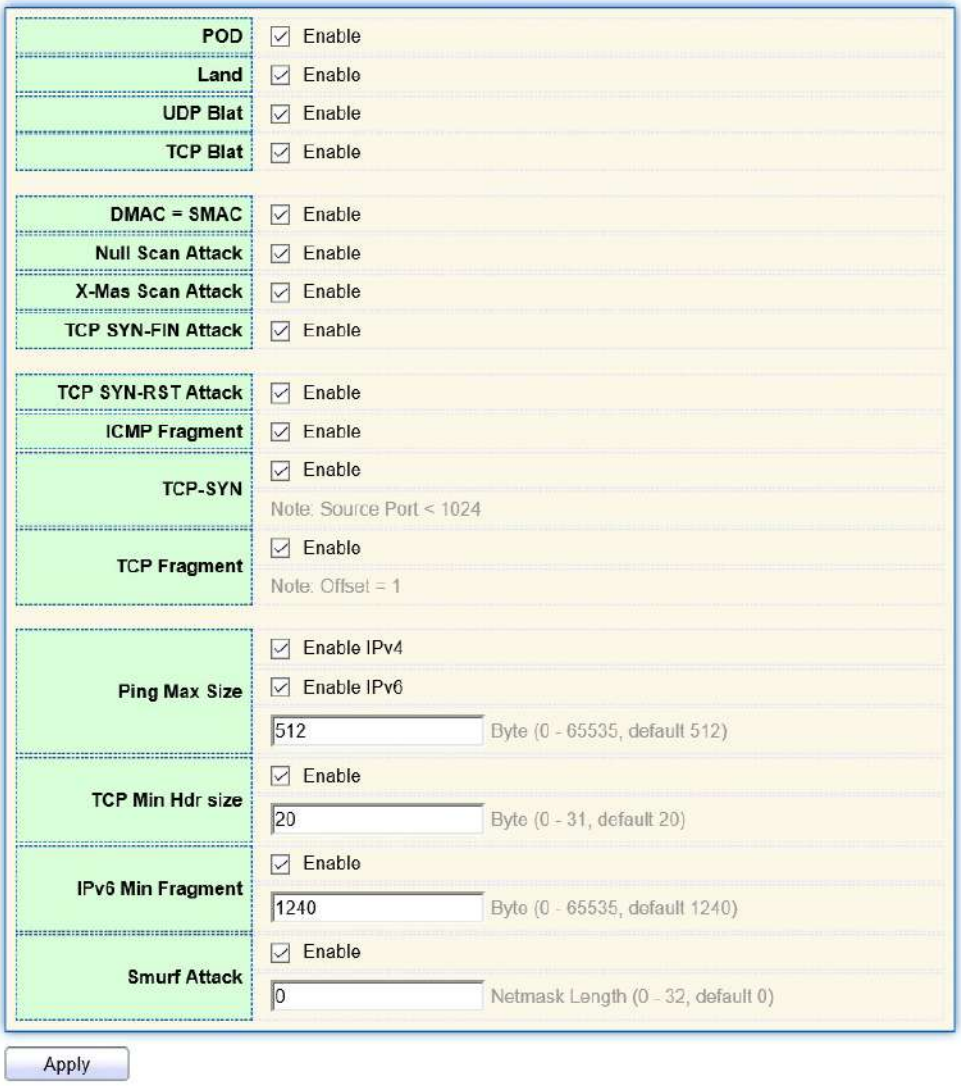


14.6 DoS

14.6.1 프로퍼티

스위치를 더욱 안전하게 만들려면 공격 저항 옵션을 활성화하십시오.

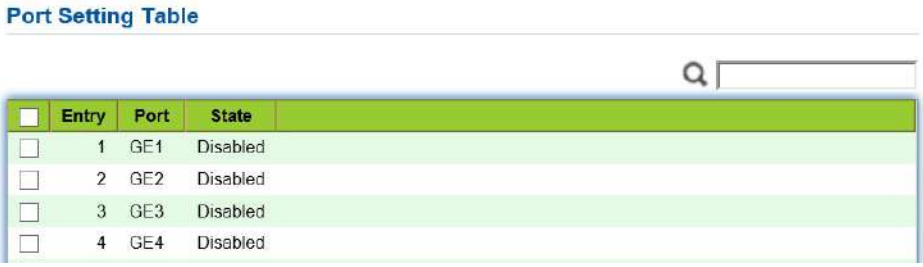
1. 다음과 같이 “DoS Global Configuration” 인터페이스에서 “Security > DoS > Property”를 클릭하세요.



14.6.2 포트 설정

DoS 공격 저항은 포트를 기준으로 활성화됩니다.

1. 다음과 같이 " Security > DoS > Port Setting "을 클릭합니다.

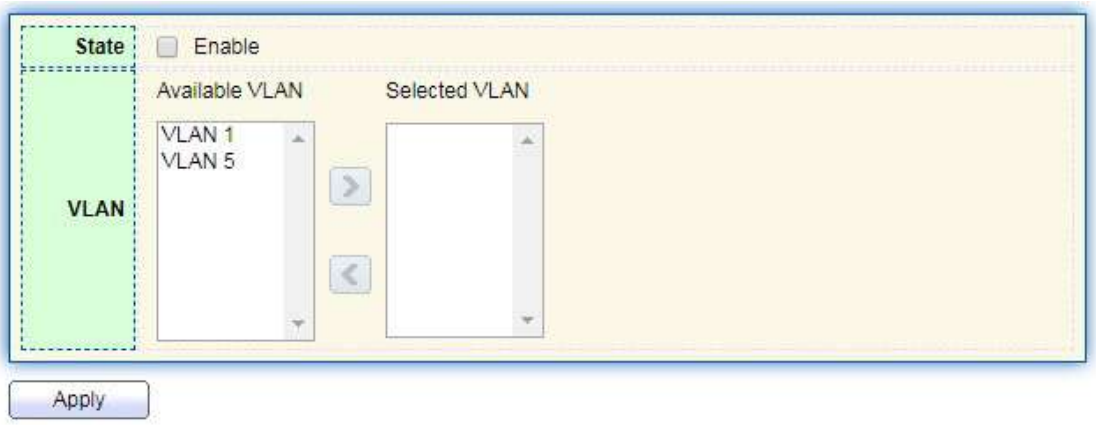


2. DoS 공격 저항 기능을 활성화 또는 비활성화하려면 다음과 같이 포트를 선택하고 "편집"하십시오.

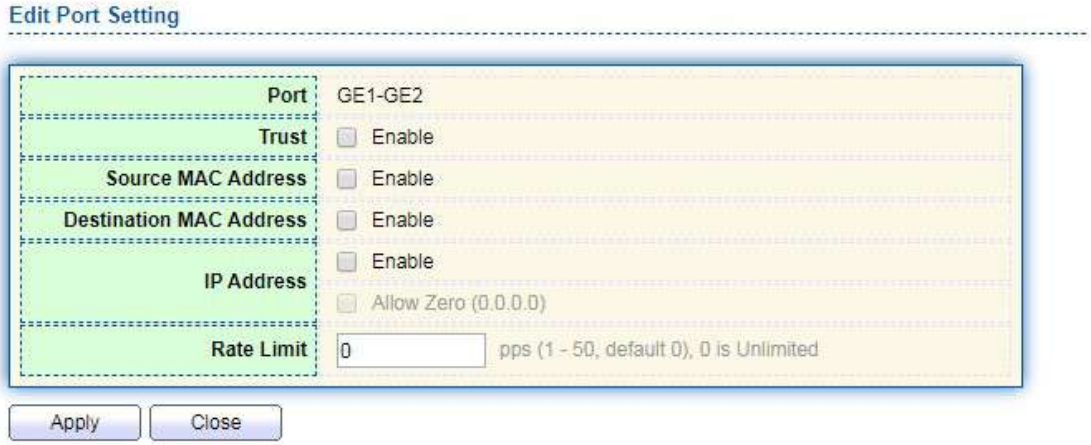
14.7 동적 ARP 검사

14.7.1 프로퍼티

1. “Security > Dynamic ARP Inspection > Property”를 클릭하고 다음과 같이 글로벌 구성 인터페이스로 들어갑니다.

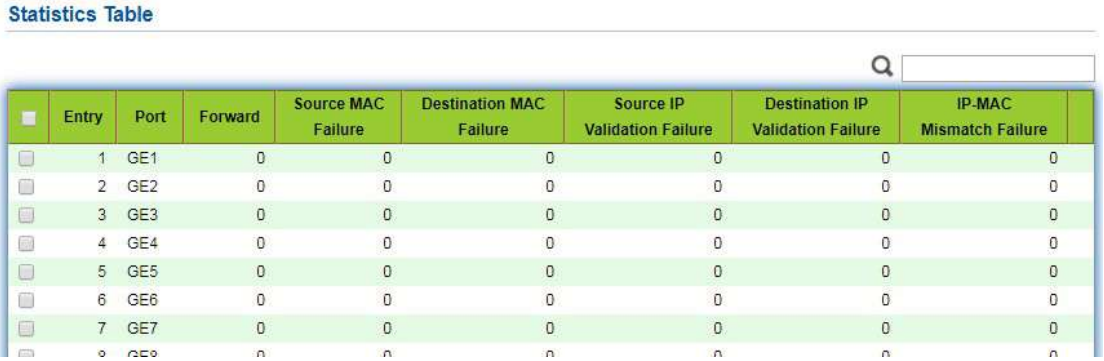


2. 포트를 선택하고 "편집"을 선택하여 다음과 같이 포트 구성 인터페이스로 들어갑니다.



14.7.2 통계

1. 다음과 같이 “Security > Dynamic ARP Inspection > Statistics”를 클릭하여 DAI 통계를 확인하세요.



Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0

14.8 DHCP 스누핑

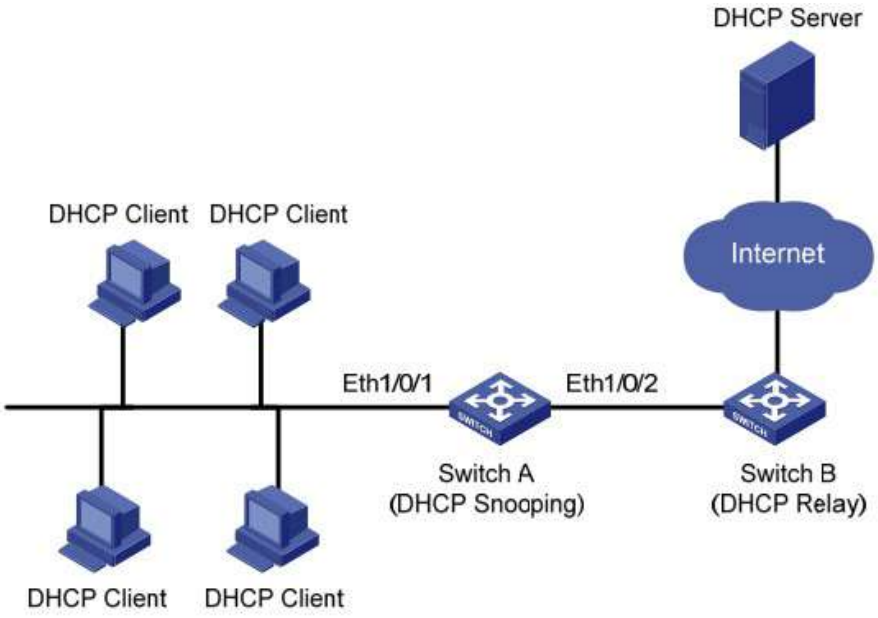
보안을 위해 네트워크 관리자는 인터넷 서핑을 하는 사용자의 IP 주소를 기록하고, DHCP 서버에서 얻은 IP 주소와 호스트의 MAC 주소가 일치하는지 확인해야 할 수 있습니다.

스위치는 네트워크 계층에서 보안 DHCP 릴레이를 통해 사용자의 IP 주소를 기록할 수 있습니다.

스위치는 데이터 링크 계층에서 DHCP Snooping 을 통해 DHCP 메시지를 모니터링하고 사용자의 IP 주소를 기록할 수 있습니다. 또한 네트워크의 개인 DHCP 서버로 인해 사용자의 IP 주소가 잘못될 수 있습니다. 사용자가 합법적인 DHCP 서버를 통해 IP 주소를 얻을 수 있도록 DHCP 스누핑 보안 메커니즘은

포트를 Trust Port 와 Untrust Port 로 나눕니다.

Trust Port 는 합법적인 DHCP 서버를 직접 또는 간접적으로 연결합니다. DHCP 클라이언트의 올바른 IP 주소를 확인하기 위해 수신된 DHCP 메시지를 전달합니다. Untrust 포트는 불법 DHCP 서버를 연결합니다. Untrust 포트의 DHCP 서버로부터 수신된 DHCPACK 및 DHCPOFFER 메시지는 잘못된 IP 주소를 방지하기 위해 폐기됩니다.



Typical Networking of DHCP Snooping

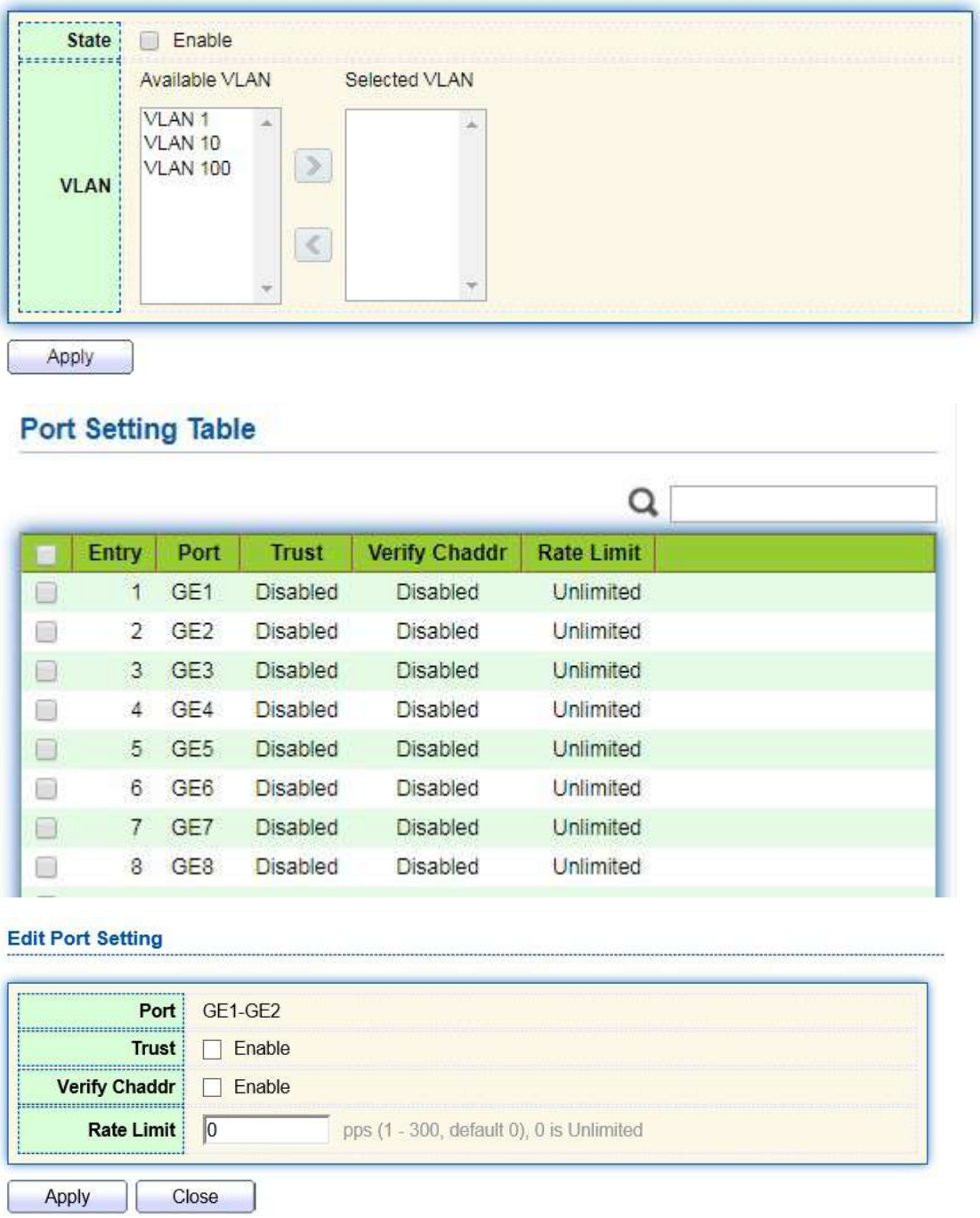
DHCP 서버에서 IP 주소와 사용자 MAC 주소를 가져오는 데는 다음 방법이 사용됩니다.

- DHCPREQUEST 메시지 스누핑
- DHCPACK 메시지 스누핑

14.8.1 프로퍼티

DHCP 스누핑 활성화

1. “Security > DHCP Snooping > Property”를 클릭하세요. DHCP 스누핑 인터페이스는 글로벌 구성과 포트 구성으로 구분됩니다. 포트 구성에서 수정할 포트를 선택하고 다음과 같이 세부 정보를 "편집"합니다.

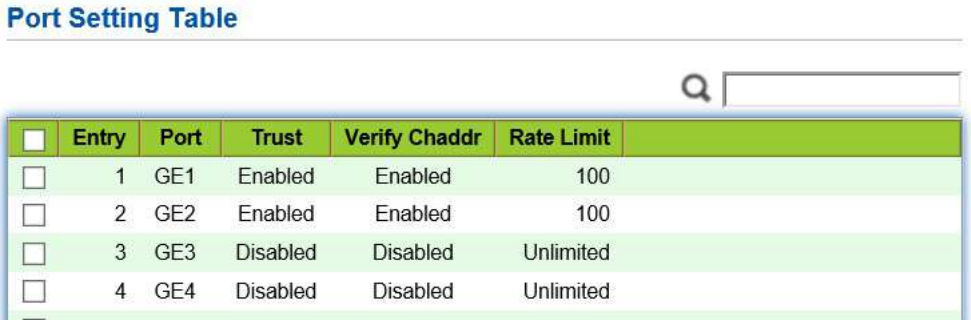


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
State	DHCP 스누핑 활성화 및 비활성화
VLAN	DHCP 스누핑의 유효한 VLAN 번호
Port	DHCP 스누핑의 포트 번호 구성
Trust	포트가 Trust Port 인지 여부

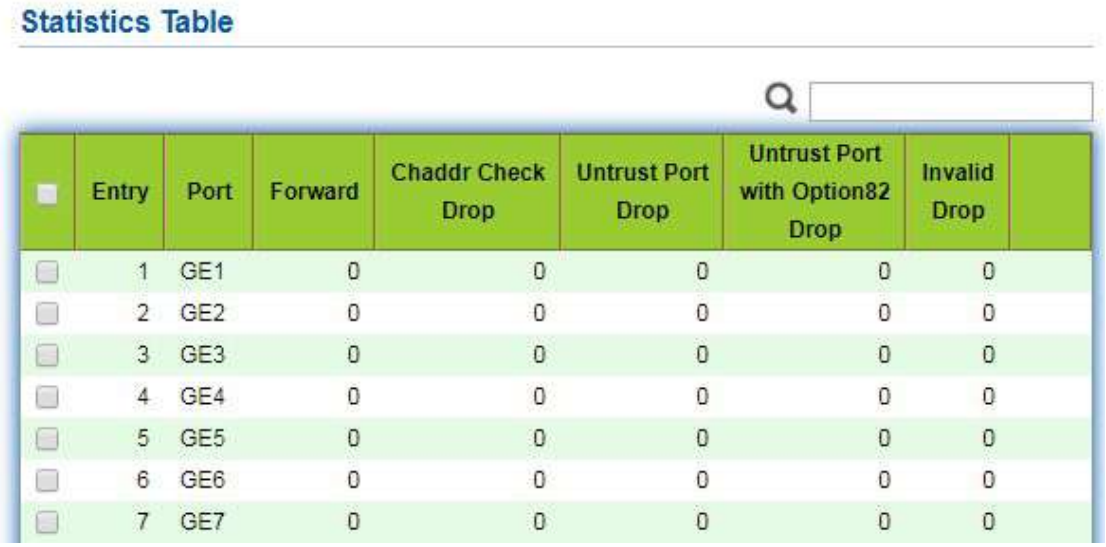
Client Address Inspection	클라이언트 주소에 대한 일관성 검사 활성화 여부
Rate Limit	포트가 속도 제한을 활성화하고 값을 구성하는지 여부

2. 해당 구성 항목을 입력합니다.
3. “적용”을 선택하고 다음과 같이 마무리합니다.



14.8.2 통계

1. 다음과 같이 " Security > Dynamic ARP Inspection > Statistics "를 클릭하여 DHCP 스누핑 통계를 확인하세요.



14.8.3 Option82 프로퍼티

네트워크의 개인 DHCP 서버로 인해 사용자가 잘못된 IP 주소를 얻을 수 있습니다. PS7024 이더넷 스위치 기반의 DHCP 스누핑 보안 메커니즘은

합법적인 DHCP 서버를 통해 IP 주소를 제공하기 위해 포트를 Trust Port 와 Untrust Port 로 구분합니다.

- Trust Port 는 합법적인 DHCP 서버를 직접 또는 간접적으로 연결합니다. 수신된 DHCP 메시지를 전달하여 DHCP 클라이언트의 올바른 IP 주소를 보장합니다.
- Untrust 포트는 불법적인 DHCP 서버를 연결합니다. 신뢰할 수 없는 포트에서 DHCP 서버가 응답한 DHCP ACK 및 DHCPOFFER 메시지는 잘못된 IP 주소를 방지하기 위해 삭제됩니다.

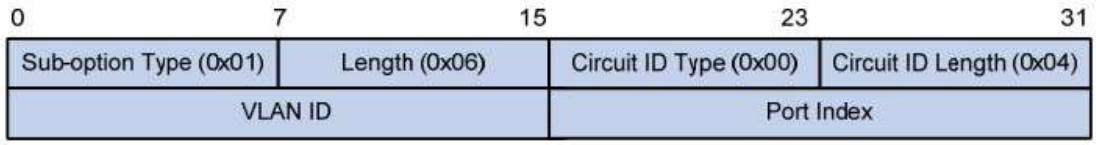
옵션 82 는 DHCP 클라이언트의 위치를 기록하는 DHCP 메시지의 릴레이 에이전트 정보 옵션입니다. DHCP 릴레이(또는 DHCP 스누핑 장치)가 DHCP 클라이언트에서 DHCP 서버로 전송된 메시지인 요청을 수신하면 관리자는 Option 82 를 추가하여 DHCP 클라이언트를 찾고 보안, 비용 등을 제어할 수 있습니다. 주소 할당에 대한 보다 유연한 접근 방식은 다음과 같습니다. IP 주소 및 기타 매개변수 할당 정책에 따라 옵션 82 를 지원하는 서버에 의해 생성됩니다.

옵션 82 에는 최대 255 개의 하위 옵션이 포함됩니다. 옵션 82 가 정의된 경우 하위 옵션을 하나 이상 정의해야 합니다. 현재 장치는 2 개의 하위 옵션을 지원합니다: 회로 ID 하위 옵션 및 원격 ID 하위 옵션

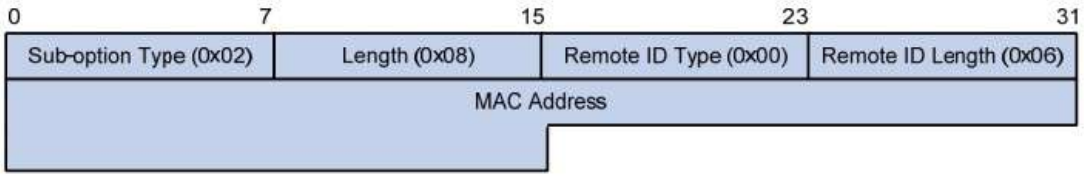
RFC 3046 이 옵션 82 옵션을 통일하지 못하기 때문에 제조업체는 일반적으로 필요에 따라 옵션을 채웁니다. DHCP 릴레이 장치로서 이더넷 스위치는 옵션 82 하위 옵션에 대한 확장 패딩 형식을 지원하며 패딩 기본값은 다음과 같습니다.

- Sub-option 1: DHCP 클라이언트가 보낸 Request 메시지를 수신하는 포트의 VLAN 번호와 포트 인덱스(포트 물리적 번호에서 1 을 뺀 값)입니다.
- Sub-option 2: DHCP 클라이언트 요청 메시지를 수신한 DHCP 릴레이 장치의 브리지 MAC 주소입니다.

Sub-option 1: DHCP 클라이언트가 보낸 Request 메시지를 수신하는 포트의 VLAN 번호와 포트 인덱스(포트 물리적 번호에서 1 을 뺀 값)는 다음과 같습니다.



Sub-option 2: DHCP 클라이언트의 DHCPREQUEST 메시지를 수신하는 DHCP 릴레이 장치의 브리지 MAC 주소입니다.



옵션 82 의 DHCP Relay 지원 메커니즘

DHCP Relay 를 통해 DHCP 클라이언트가 DHCP 서버로부터 IP 주소를 획득하는 과정은 기본적으로 DHCP 서버에서 직접 IP 주소를 얻는 과정과

동일합니다. 발견, 제공, 선택 및 검증 단계가 필수적입니다. DHCP 릴레이의 지원 메커니즘은 다음과 같이 소개됩니다.

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

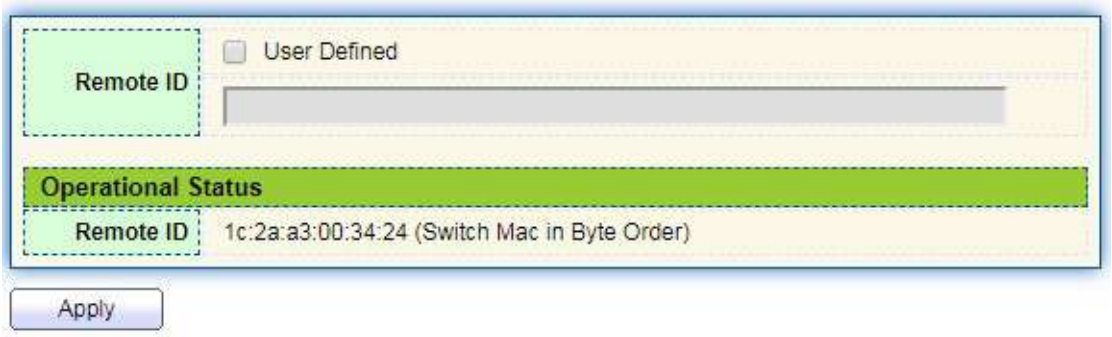
- 기존 옵션 82 메시지의 경우 DHCP 릴레이는 구성 정책(폐기, 릴레이 옵션 82 로 교체, 원래 옵션 82 유지)에 따라 처리한 후 DHCP 서버로 전달됩니다.
- 옵션 82 가 없는 메시지의 경우 DHCP 릴레이는 새 메시지를 DHCP 서버에 추가하고 전달합니다.

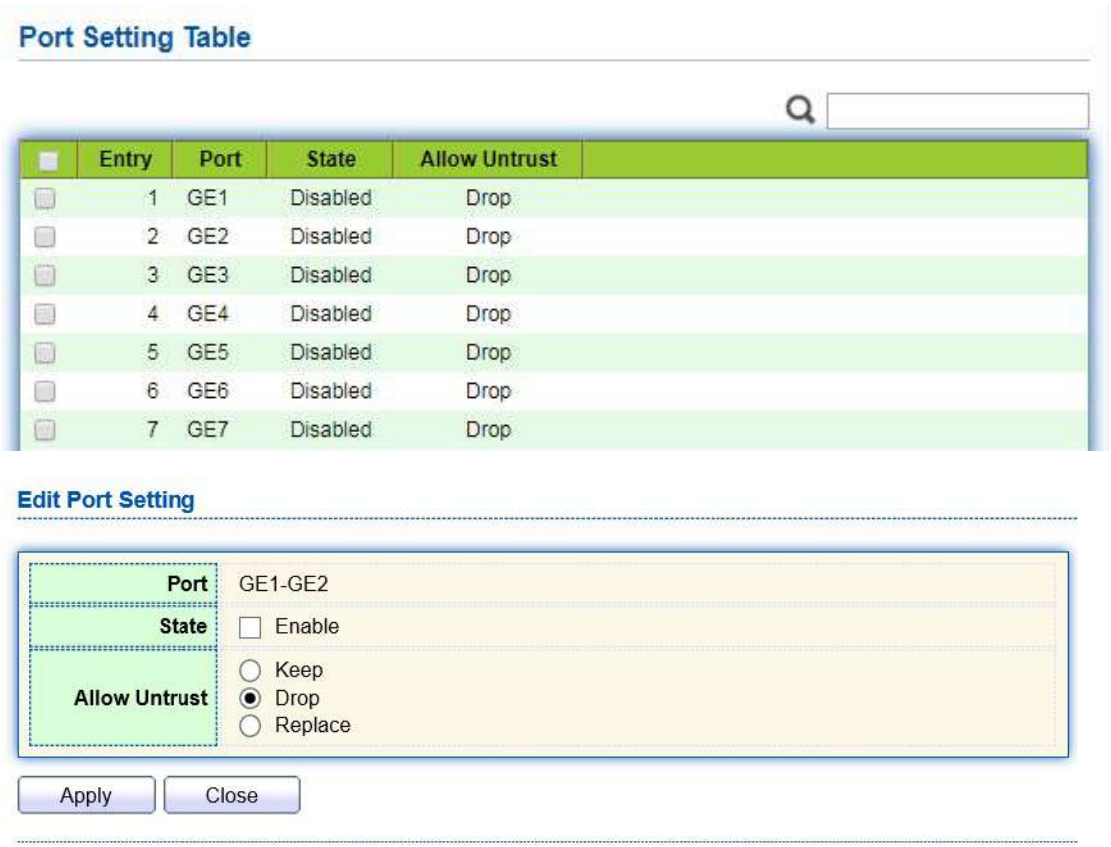
(2) DHCP 릴레이는 DHCP 서버로부터 받은 응답 메시지에서 옵션 82 를 떼어낸 후 DHCP 구성 정보가 포함된 메시지를 DHCP 클라이언트로 전달합니다.

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

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

1. “Security > DHCP Snooping > Option82 Property”를 클릭하세요. 전역 및 포트 구성이 포함되어 있습니다. 구성할 포트를 선택하고 다음과 같이 세부 정보를 "편집"합니다.



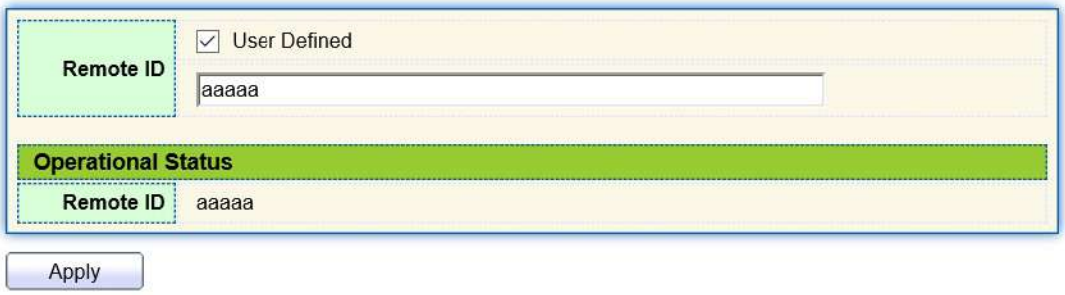


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Remote ID	옵션 82(예: 사용자 정의 XXXX)의 원격 ID 필드를 입력합니다.
Port	옵션 82 의 포트번호 활성화 여부
Untrust Port Access	Untrust 포트는 옵션 82 가 활성화된 메시지를 처리합니다. Maintaining: 메시지의 옵션 82 를 변경하지 않고 그대로 두고 전달하세요. Discarding: 메시지를 삭제합니다. Replacing: 회로 ID 구성에 따라 메시지의 옵션 82 필드를 대체하고 전달합니다.

옵션 82 필드는 회로 ID 또는 원격 ID 하위 옵션을 독립적으로 구성합니다.
특정 순서 없이 개별적으로 또는 동시에 구성할 수 있습니다.
사용자 표시줄에서 DHCP 옵션 82 를 구성해야 합니다. 그렇지 않으면 DHCP 서버로 전송된 DHCP 메시지에 옵션 82 가 전달되지 않습니다.
DHCP 서버로부터 DHCP 응답 메시지를 수신할 때 옵션 82 가 포함된 메시지는 해당 필드를 삭제한 후 전달되고, 메시지에 옵션 82 가 포함되어 있지 않은 경우에는 직접 전달됩니다.

2. 해당 구성 항목을 입력합니다.
3. “적용”을 선택하고 다음과 같이 마무리합니다.



Port Setting Table

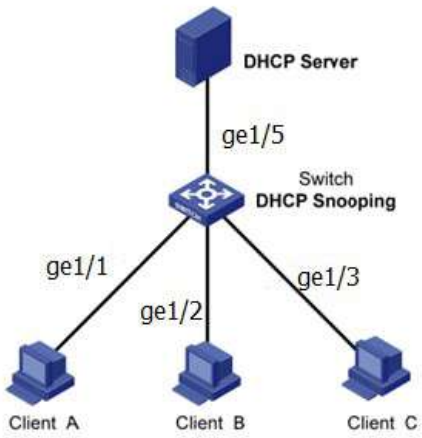
Entry	Port	State	Allow Untrust
1	GE1	Enabled	Replace
2	GE2	Enabled	Replace
3	GE3	Enabled	Replace
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop

DHCP 스누핑 일반적인 구성 그림.

아래 그림과 같이 스위치 포트 GE1-5 는 DHCP 서버에 연결되고, 포트 GE1-1, 2, 3 은 각각 DHCP 클라이언트 A, B, C 에 연결됩니다.

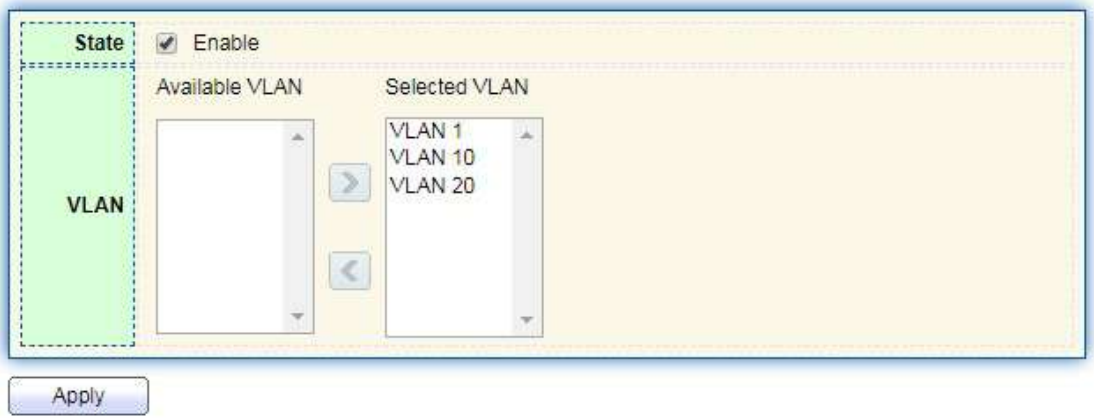
- 스위치에서 DHCP 스누핑을 활성화합니다.
- GE1-5 를 DHCP 스누핑의 신뢰 포트로 설정합니다.
- 스위치에서 옵션 82 지원 기능을 활성화합니다. 포트를 통해 흐르는 GE1-3 메시지의 경우 Circuit ID 와 Remote ID 의 기본 구성에 따라 Option 82 를 입력합니다.

Network Diagram



Configure DHCP snooping to support Option 82

1. 스위치의 DHCP 스누핑을 활성화합니다. 탐색 바에서 “Security > DHCP Snooping > Property”를 클릭하여 다음과 같이 기능을 활성화하세요.



2. GE1-5 를 DHCP 스누핑의 신뢰 포트로 설정하고 해당 구성을 입력한 후 다음과 같이 "편집"합니다.

3. 옵션 82 로 사용자 정의 원격 ID 를 설정할 수 있도록 GE3 포트를 구성합니다. “Security > DHCP Snooping > Option82 Property”를 클릭하여 포트를 확인하고 구성합니다. "적용"하고 다음과 같이 완료합니다.

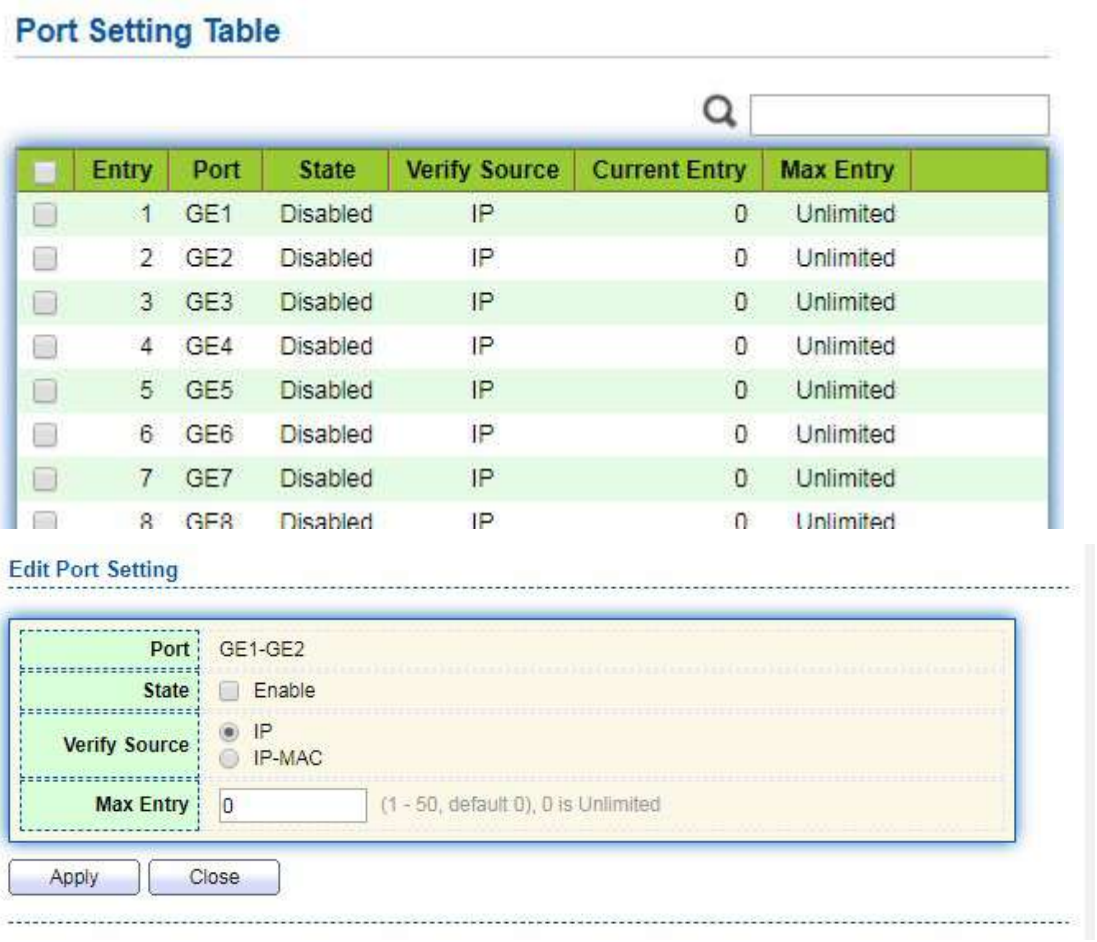
4. 회로 ID가 옵션 82로 설정될 수 있도록 포트 GE3에서 구성합니다. “Security > DHCP Snooping > Option82 Circuit ID”를 클릭하여 포트를 구성합니다. "적용"하고 다음과 같이 완료합니다.

14.9 IP 소스 가드

IPSG(IP Source Guard)는 IP/Mac 기반의 포트 트래픽 필터링 기술로, LAN에서 IP 주소 스푸핑 공격을 방지할 수 있습니다. IPSG는 레이어 2 네트워크에 있는 단말 장치의 IP 주소가 탈취되지 않도록 보장할 수 있으며, 승인되지 않은 장치가 네트워크에 액세스하거나 자체 지정된 IP 주소를 통해 네트워크를 공격할 수 없도록 보장할 수 있습니다.

14.9.1 포트 설정

1. " Security > IP Source Guard > Port Setting "을 클릭하고 다음과 같이 포트 구성 인터페이스로 들어갑니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 목록
State	IPSG 활성화 또는 비활성화
Verify Source	기본 IP 소스 가드 필터 소스 IP 주소입니다. “IP-MAC”은 소스 IP 주소뿐만 아니라 소스 MAC 주소도 필터링합니다.
Max Entry	허용되는 최대 포트 수

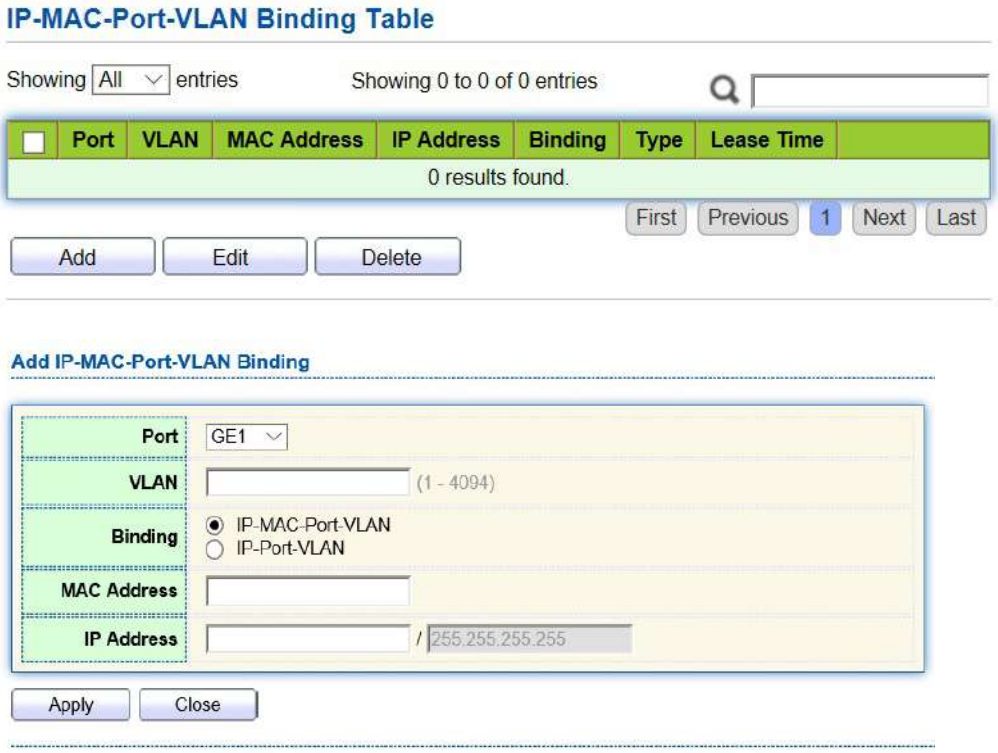
14.9.2 IMPV 바인딩

DHCP 네트워크에서는 정적으로 IP 주소를 획득한 사용자(DHCP 가 아닌 사용자)가 DHCP 서버를 모방하거나 DHCP 요청 메시지를 구성하는 등의 방법으로 네트워크를 공격할 수 있습니다. 합법적인 DHCP 사용자는 네트워크를 정상적으로 사용하는 경우 보안 위험에 노출될 수 있습니다.

DHCP 스누핑 바인딩 테이블에 의해 생성된 인터페이스를 기반으로 정적 MAC 항목을 활성화하면 이러한 공격을 방지할 수 있습니다. 그런 다음 장치는

모든 DHCP 사용자에 해당하는 DHCP 스누핑 바인딩 테이블을 기반으로 자동으로 명령을 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 통과할 수 있고 나머지는 삭제됩니다.

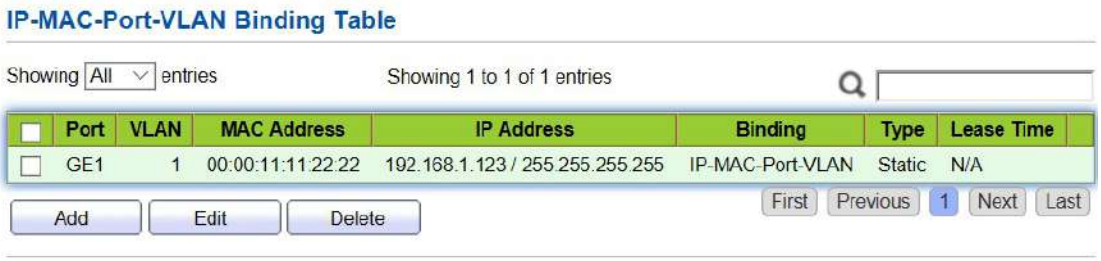
1. " Security > IP Source Guard > IMPV Binding""을 클릭하고 다음과 같이 IP-MAC-Port-VLAN 의 새 바인딩 그룹을 "추가"합니다.



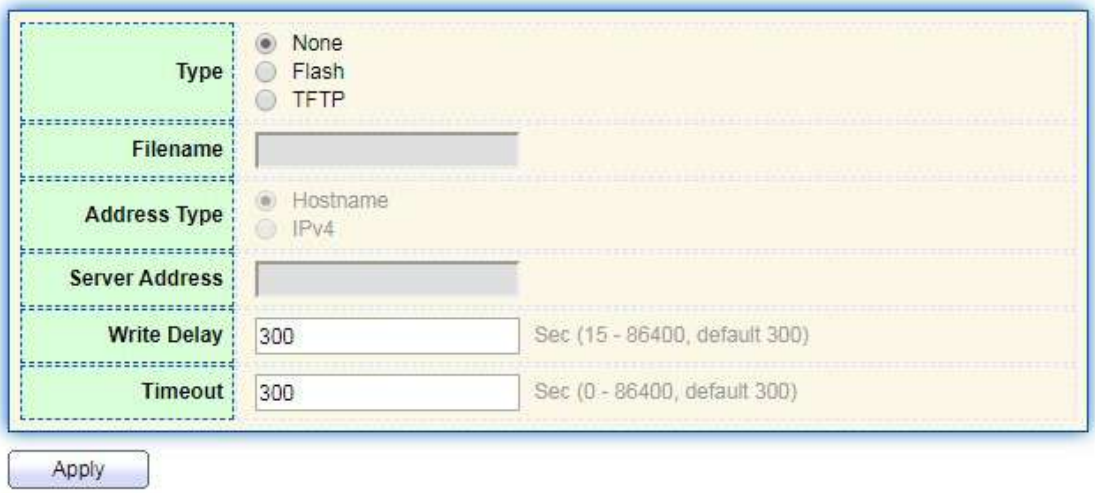
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	바인딩 그룹의 포트 번호
VLAN	VLAN ID 바인딩
Binding	IPMV 와 IPV 의 바인딩 관계를 선택합니다.
MAC Address	MAC 주소 바인딩
IP Address	IP 주소 바인딩

2. 해당 구성 항목을 입력합니다.
3. "적용"을 선택하고 다음과 같이 마무리합니다.



4. " Security > IP Source Guard > Save Database "을 클릭하고 다음과 같이 데이터베이스 인터페이스를 입력합니다.



15 ACL

네트워크 규모 확장 및 흐름 탑재로 네트워크 보안 제어 및 대역폭 할당의 위치가 강화됩니다. 패킷 필터링은 불법 사용자의 접속을 방지하고 흐름을 제어하며 네트워크 자원을 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 결정된 정책에 따라 해당 메시지의 흐름이 허용되거나 금지됩니다.

ACL 에 의해 정의된 패킷 일치 규칙은 QoS 흐름 분류 규칙 정의와 같이 흐름 구별이 필요한 다른 기능에서도 참조될 수 있습니다.

ACL 은 일치 규칙 및 처리 방법을 설정하여 패킷을 필터링할 수 있습니다. ACL 은 패킷에 적용되는 허가 및 거부 조건의 모음입니다. 인터페이스가 패킷을 수신하면 스위치는 필드와 ACL 을 비교하여 지정된 표준에 따라 허용되는 패킷과 거부되는 패킷을 결정합니다. ACL 은 소스/대상 MAC 주소, 소스/대상 IP 주소, 포트 번호 등 일치 조건을 기준으로 패킷을 분류합니다. ACL 은 소스/대상 주소,

포트 번호 등 일치 조건에 따라 패킷을 분류합니다. ACL 은 응용 목적에 따라 다음 범주로 나눌 수 있습니다.

기본 IP ACL 은 패킷의 소스 IP 주소만을 기반으로 규칙을 구성합니다. ACL ID 범위는 100~999 입니다. 고급 IP ACL 은 패킷의 소스/대상 IP 주소, IP 가 전달하는 프로토콜 유형, 프로토콜 특성과 같은 레이어 3 또는 4 정보에 따라 규칙을 준비합니다. ACL ID 범위는 100~999 입니다.

L2 ACL: 패킷의 소스/대상 MAC 주소, 802.1p 우선순위, 프로토콜 유형과 같은 L2 정보에 따라 규칙이 만들어집니다. ACL ID 의 범위는 1 부터 99 까지입니다.

15.1 MAC ACL

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

1. 다음과 같이 탐색 표시줄에서 “ACL > MAC ACL”을 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
ACL Name	MAC ACL 규칙 이름 지정

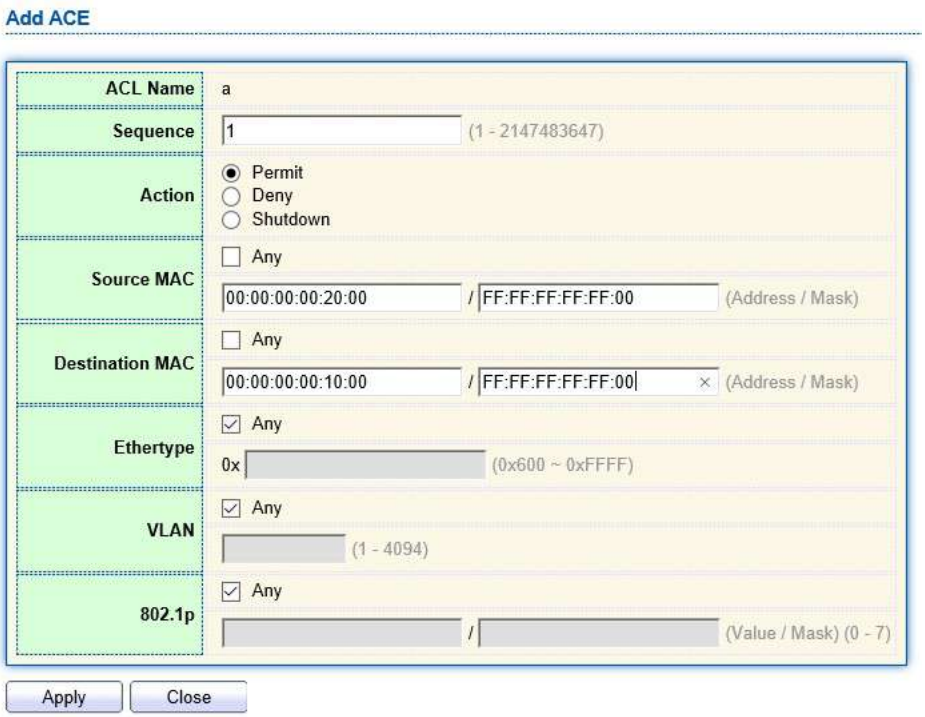
2. 탐색 모음에서 "ACL > MAC ACE"를 클릭하고 다음과 같이 ACL 이름을 "추가"합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
ACL Name	ACL 규칙 목록은 MAC ACL 구성을 기반으로

	준비됩니다.

3. 해당 구성 항목을 입력합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
ACL Name	ACL 규칙 목록은 MAC ACL 구성을 기반으로 준비됩니다.
Sequence	MAC ACL 범위는 1~2,147,483,647 입니다.
Action	ACL 작업은 "허용", "거부" 및 "종료"로 구분됩니다.
Source MAC	ACL 규칙의 원본 MAC 주소와 마스크를 H.H.H.H.H.H 형식으로 입력하세요. MAC 주소를 나타내려면 "Any"를 선택하십시오.
Destination MAC	H.H.H.H.H.H 형식으로 대상 MAC 주소와 ACL 규칙 마스크를 입력합니다. MAC 주소를 나타내려면 "Any"를 선택하십시오.
EtherType	0 x 600 에서 0 x FFFF 범위의 ACL 규칙의 이더넷 유형을 입력하고 모든 유형을 나타내려면 "Any"를 선택하십시오.
VLAN	1~4,094 범위의 ACL 규칙의 VLAN 을 입력하고 모든 VLAN 을 나타내려면 "Any"를 선택합니다.
802.1p	VLAN 우선순위와 1~7 범위의 ACL 규칙 마스크를 입력하고 VLAN 우선순위를 나타내려면 "Any(모두)"를 선택합니다.

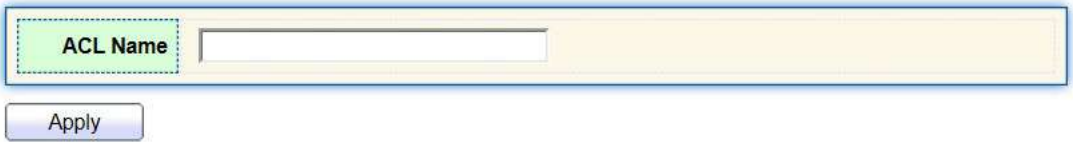
4. “적용”을 선택하고 다음과 같이 마무리합니다.

15.2 IPv4 ACL

IPv4 기반 ACL(기본 IP ACL)은 패킷의 소스 IP 주소에 대해서만 규칙을 작성합니다. ACL ID 범위는 100~999 입니다.

고급 IP ACL 규칙은 패킷의 소스/대상 IP 주소, IP 가 전달하는 프로토콜 유형, 프로토콜 특성과 같은 레이어 3 또는 4 정보에 따라 만들어집니다. ACL ID 범위는 100~999 입니다.

1. 다음과 같이 탐색 표시줄에서 “ACL > IPv4 ACL”을 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

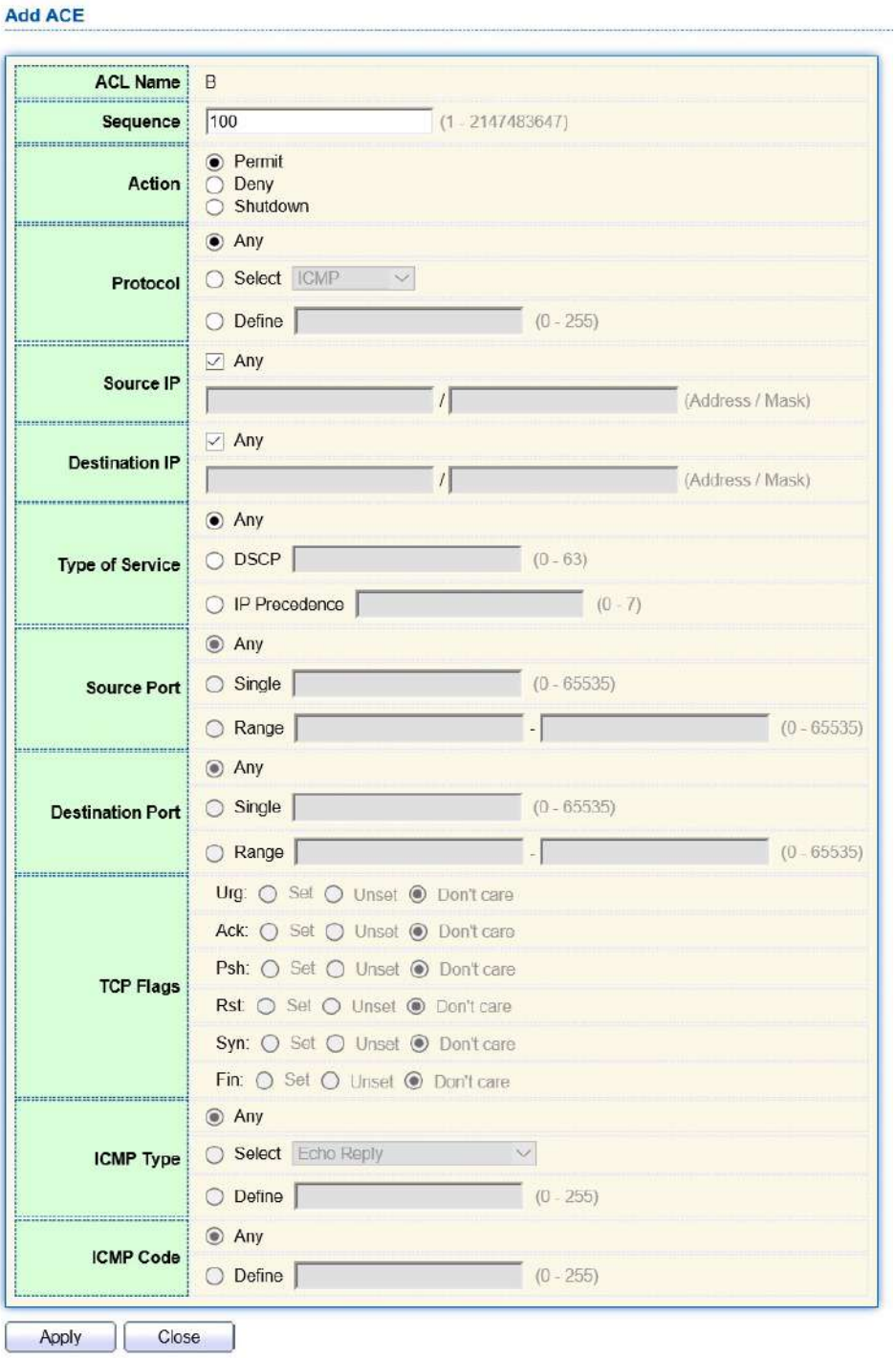
설정 항목	설명
ACL Name	IPv4 ACL 규칙 이름 지정

2. 탐색 모음에서 "ACL > IPv4 ACE"를 클릭하고 다음과 같이 ACL 이름을 "추가"합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
ACL Name	ACL 규칙 목록은 IPv4 ACL 구성을 기반으로 만들어집니다.

3. 해당 구성 항목을 입력합니다.



인터페이스 데이터는 다음과 같습니다.

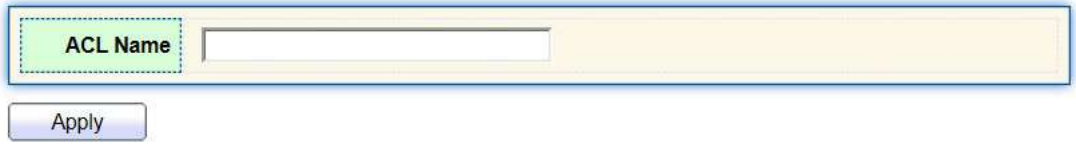
설정 항목	설명
ACL Name	ACL 규칙 목록은 IPv4 ACL 구성을 기반으로 만들어집니다.
Sequence	IPv4 ACL 범위는 1~2,147,483,647 입니다.
Action	ACL 작업은 "허용","거부" 및 "종료"로 구분됩니다.

Protocol	ICMP, TCP, UDP 등의 프로토콜 유형을 선택해야 합니다. 모든 프로토콜을 나타내려면 "모두"를 선택하십시오.
Source IP	ACL 규칙의 소스 IP 와 마스크를 입력합니다. 모든 소스 IP 를 나타내려면 "모두"를 선택합니다.
Destination IP	ACL 규칙의 대상 IP 와 마스크를 입력합니다. 대상 IP 를 나타내려면 "모두"를 선택합니다.
Type of Service	DSCP(0-63) 및 IP 우선순위(0-7)와 같은 ACL 규칙의 서비스 유형을 입력합니다. 모든 서비스 유형을 나타내려면 "모두"를 선택하십시오.
Source Port	단일 포트 번호 또는 범위 세그먼트(0-65,535)와 같은 ACL 규칙의 소스 포트를 입력합니다. 모든 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 선택합니다.
TCP Flags	URG, ACK, PSH, RST, SYN, FIN 과 같은 ACL 규칙의 TCP 플래그를 "설정", "설정 해제" 및 "상관 없음"과 같은 작업과 함께 입력합니다.
ICMP Type	ACL 규칙의 ICMP 메시지 유형을 입력합니다. ICMP 유형을 나타내려면 "모두"를 선택합니다.
ICMP Code	ACL 규칙의 ICMP 코드 값을 입력합니다. 모든 필드 값을 나타내려면 "모두"를 선택합니다.

4. “적용”을 선택하고 다음과 같이 마무리합니다.

15.3 IPv6 ACL

1. 다음과 같이 탐색바에서 “ACL > IPv6 ACL”을 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

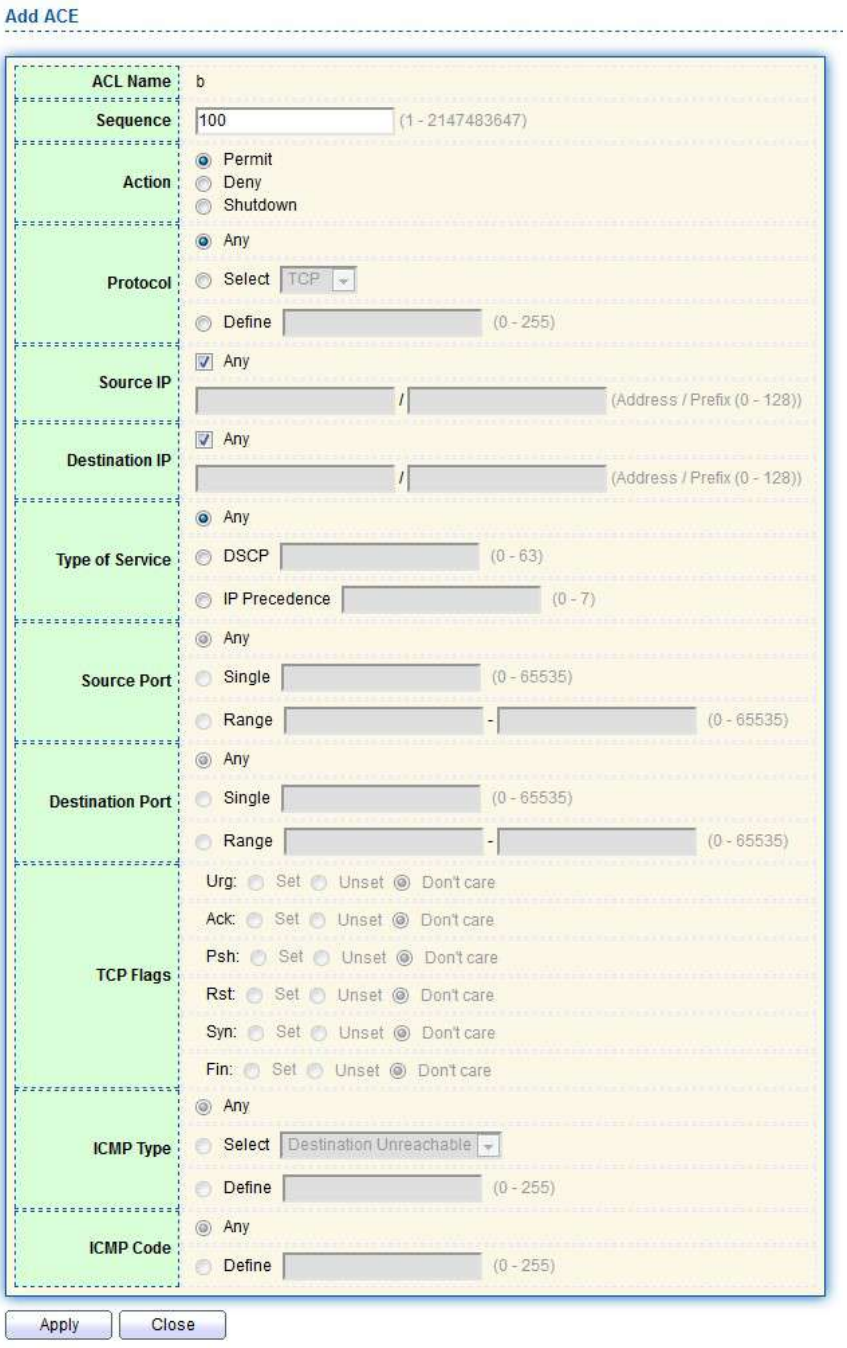
설정 항목	설명
ACL Name	Pv6 ACL 규칙 이름 지정

2. 탐색 모음에서 "ACL > IPv6 ACE"를 클릭하고 다음과 같이 ACL 이름을 "추가"합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
ACL Name	ACL 규칙 목록은 IPv6 ACL 구성을 기반으로 만들어집니다.

3. 해당 구성 항목을 입력합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
ACL Name	ACL 규칙 목록은 IPv6 ACL 구성을 기반으로 만들어집니다.
Sequence	IPv6 ACL 범위는 1~2,147,483,647 입니다.
Action	ACL 작업은 "허용","거부" 및 "종료"로 구분됩니다.
Protocol	ICMP, TCP, UDP 등의 프로토콜 유형을 선택해야 합니다. 모든 프로토콜을 나타내려면 "모두"를 선택하십시오.

Source IP	ACL 규칙의 소스 IP 와 마스크를 입력합니다. 모든 소스 IP 를 나타내려면 "모두"를 선택합니다.
Destination IP	ACL 규칙의 대상 IP 와 마스크를 입력합니다. 대상 IP 를 나타내려면 "모두"를 선택합니다.
Type of Service	DSCP(0-63) 및 IP 우선순위(0-7)와 같은 ACL 규칙의 서비스 유형을 입력합니다. 모든 서비스 유형을 나타내려면 "모두"를 선택하십시오.
Source Port	단일 포트 번호 또는 범위 세그먼트(0-65,535)와 같은 ACL 규칙의 소스 포트를 입력합니다. 모든 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 선택합니다.
TCP Flags	URG, ACK, PSH, RST, SYN, FIN 과 같은 ACL 규칙의 TCP 플래그를 "설정", "설정 해제" 및 "상관 없음"과 같은 작업과 함께 입력합니다.
ICMP Type	ACL 규칙의 ICMP 메시지 유형을 입력합니다. ICMP 유형을 나타내려면 "모두"를 선택합니다.
ICMP Code	ACL 규칙의 ICMP 코드 값을 입력합니다. 모든 필드 값을 나타내려면 "모두"를 선택합니다.

4. “적용”을 선택하고 다음과 같이 마무리합니다.

15.4 ACL 바인딩

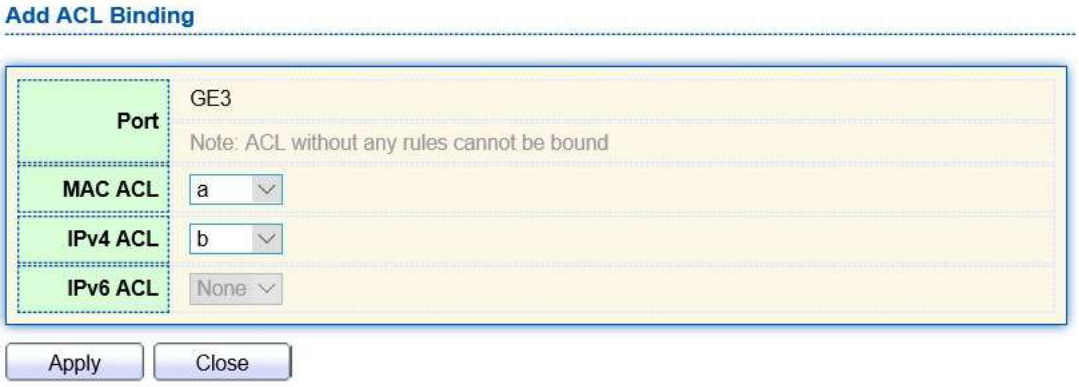
목록이 생성되면 각 필수 인터페이스에 바인딩되어야 합니다.

1. 다음과 같이 네비게이션 바에서 “ACL > ACL Binding”을 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
MAC ACL	포트에 바인딩된 MAC ACL 이름
IPv4 ACL	포트에 바인딩된 IPv4 ACL 이름(IPv6 ACL 과 상호 배타적)
IPv6 ACL	포트에 바인딩된 IPv6 ACL 이름(IPv4 ACL 과 상호 배타적)

2. 생성된 MAC ACL a, IPv4 ACL b, IPv6 ACL c 를 예로 들어 해당 구성 항목을 입력합니다.
3. “적용”을 선택하고 다음과 같이 마무리합니다.



16 QoS

QoS(서비스 품질)는 서비스 제공업체가 고객 요구를 충족하는 능력과 인터넷을 통해 패킷을 전송하는 능력을 평가합니다. 다양한 측면을 기반으로 다양한 서비스를 평가할 수 있습니다. QoS 는 일반적으로 대역폭, 지연, 지연 변화, 전송 중 패킷 손실률 등 핵심 요구 사항을 지원하는 서비스 기능을 평가하는 것을 의미합니다. 처리량이라고도 하는 대역폭은 Kbit/s 단위로 특정 기간 내의 평균 비즈니스 흐름을 나타냅니다. 지연은 네트워크를 통해 비즈니스가 흐르는 데 필요한 평균 시간을 나타냅니다. 네트워크 장치의 경우 일반적인 지연 요구

사항 수준은 다음과 같습니다. 두 가지 지연 수준이 있습니다. 즉, 우선순위 대기열의 예약 방법을 통해 우선순위가 높은 비즈니스에 최대한 빨리 서비스를 제공할 수 있고, 우선순위가 낮은 비즈니스는 그 이후에 서비스를 받을 수 있습니다. 지연 변동은 네트워크를 통해 흐르는 비즈니스의 시간 변화를 의미합니다. 패킷 손실률은 전송 중 손실된 비즈니스 흐름의 비율을 나타냅니다. 현대 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 처리하며 안정성, 전송 지연 또는 기타 성능을 보장하지 않고 메시지를 대상으로 전송하기 위해 최선을 다합니다.

급변하는 IP 네트워크 속에서 새로운 애플리케이션이 계속해서 생겨나면서 네트워크 서비스 품질은 지속적으로 향상되고 있습니다. 예를 들어 VoIP, 비디오 및 기타 지연에 민감한 서비스는 메시지 전송 지연에 대해 더 높은 기준을 설정했습니다. 단기간에 메시지를 전송하는 것이 일반적인 추세입니다. 다양한 요구 사항을 가진 음성, 비디오 및 데이터 서비스를 지원하려면 네트워크에서 비즈니스 유형을 식별하고 해당 서비스를 제공해야 합니다.

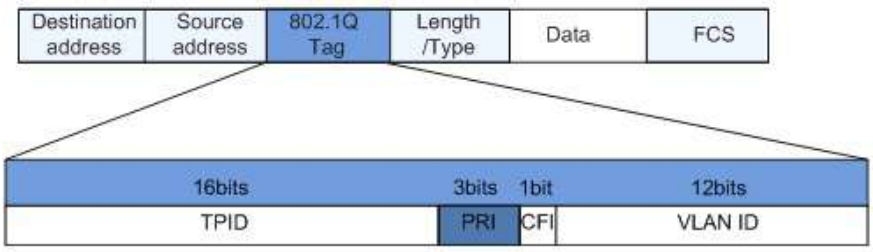
비즈니스 유형을 구별하는 능력은 해당 서비스를 제공하기 위한 전제 조건이므로 기존의 최선을 다하는 서비스는 더 이상 애플리케이션 요구 사항을 충족할 수 없습니다. 따라서 QoS 가 발생합니다. 네트워크 정체를 방지 및 처리하고 패킷 손실률을 줄이기 위해 네트워크 흐름을 조절합니다. 동시에 사용자는 전용 대역폭을 즐길 수 있고 기업은 서비스 품질을 향상시켜 네트워크 서비스 용량을 완벽하게 만들 수 있습니다.

QoS 우선순위는 메시지 유형에 따라 다릅니다. 예를 들어 VLAN 메시지는 CoS(서비스 클래스) 필드라고도 하는 802.1p 를 사용하는 반면, IP 메시지는 DSCP 를 사용합니다. 우선순위를 유지하기 위해서는 메시지가 네트워크를 통해 흐를 때 다양한 네트워크와 연결된 게이트웨이에서 이러한 필드를 매핑해야 합니다.

VLAN 프레임 헤더의 802.1p 우선순위

일반적으로 VLAN 프레임은 레이어 2 장치 간에 상호 작용합니다. VLAN 프레임 헤더의 PRI 필드(예: 802.1p 우선 순위) 또는 CoS 필드는 IEEE 802.1Q 의 정의에 따라 서비스 품질 요구 사항을 식별합니다.

VLAN 프레임의 802.1p 우선순위

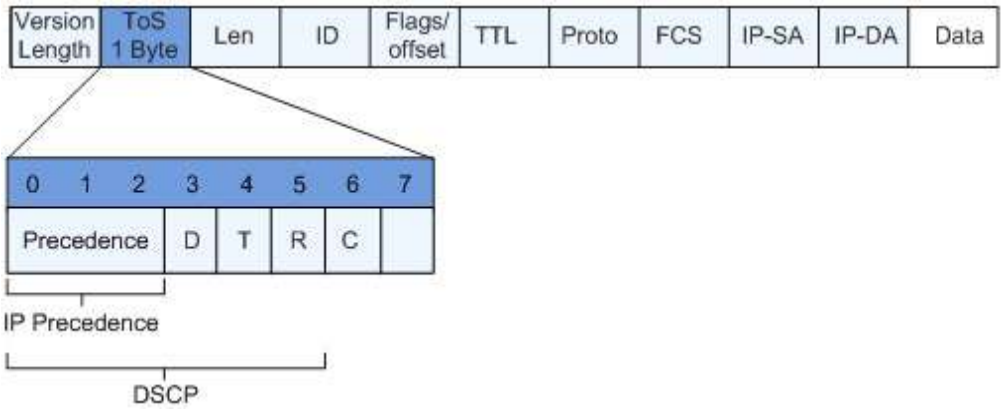


802.1Q 헤더에는 3 비트 PRI 필드가 포함되어 있습니다. PRI 필드는 7 부터 0 까지 높음부터 낮음까지의 비즈니스 우선순위에 대한 8 개의 CoS 를 정의합니다.

IP 우선순위/DSCP 필드

RFC791 정의에 따르면 IP 메시지 헤더의 ToS(Type of Service) 도메인은 8 비트로 구성됩니다. 그 중 다음과 같은 3 비트 길이의 Precedence 필드는 IP 메시지 우선순위를 식별한다.

IP 우선순위/DSCP 필드



0~2 비트는 7~0, 높은 수준에서 낮은 수준까지의 8 가지 메시지 전송 우선 순위를 나타내는 우선 순위 필드입니다. 레벨 7 또는 6 은 일반적으로 네트워크 제어 통신 라우팅 또는 업데이트를 위해 예약된 가장 높은 우선 순위입니다. 사용자 수준 애플리케이션은 수준 0~5 에만 액세스할 수 있습니다.

ToS 도메인에는 우선 순위 필드 외에도 D, T 및 R 비트도 포함됩니다. D 비트는 지연 요구 사항을 나타냅니다(정상 지연의 경우 0, 낮은 지연의 경우 1). T 비트는 처리량을 나타냅니다(일반 처리량은 0, 높은 처리량은 1). R 비트는 신뢰성을 나타냅니다(0 은 보통 신뢰성, 1 은 높은 신뢰성). ToS 도메인은 6 비트와 7 비트를 예약합니다.

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

DS 필드의 처음 6 비트(0~5 비트)는 DSCP(DS Code Point)를 구분하고 상위 2 비트(6~7 비트)는 예약되어 있습니다. 하위 3 비트(0~2 비트)는 CSCP(Class Selector Code Point)로, 동일한 CSCP 값은 동일한 클래스의 DSCP 를 나타냅니다. DS 노드는 DSCP 값에 따라 해당 PHB(Per-Hop Behavior)를 선택합니다.

16.1 일반

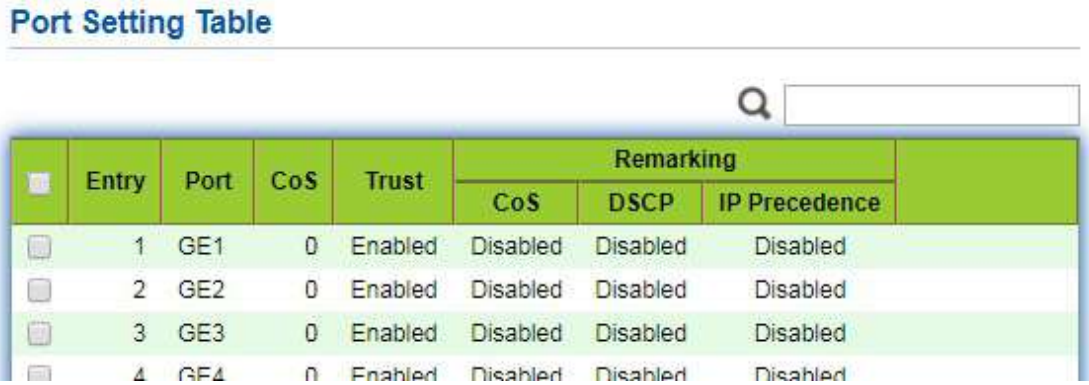
16.1.1 프로퍼티

동시에 메시지 간 자원 사용권 경쟁으로 인한 네트워크 정체는 일반적으로 대기열 스케줄링을 통해 해결되므로 간헐적인 정체를 방지할 수 있습니다. 대기열 스케줄링 기술에는 SP(Strict-Priority), WFQ(Weighted Fair Queue), WRR(Weighted Round Robin) 및 DRR(역시 RR 기술에서 확장된 Deficit Round

Robin)이 포함됩니다.

글로벌 및 포트 스케줄링 구성에 대한 가이드

1. 다음과 같이 네비게이션 바에서 “QoS > General > Property”를 클릭하세요.



글로벌 구성의 인터페이스 데이터는 다음과 같습니다.

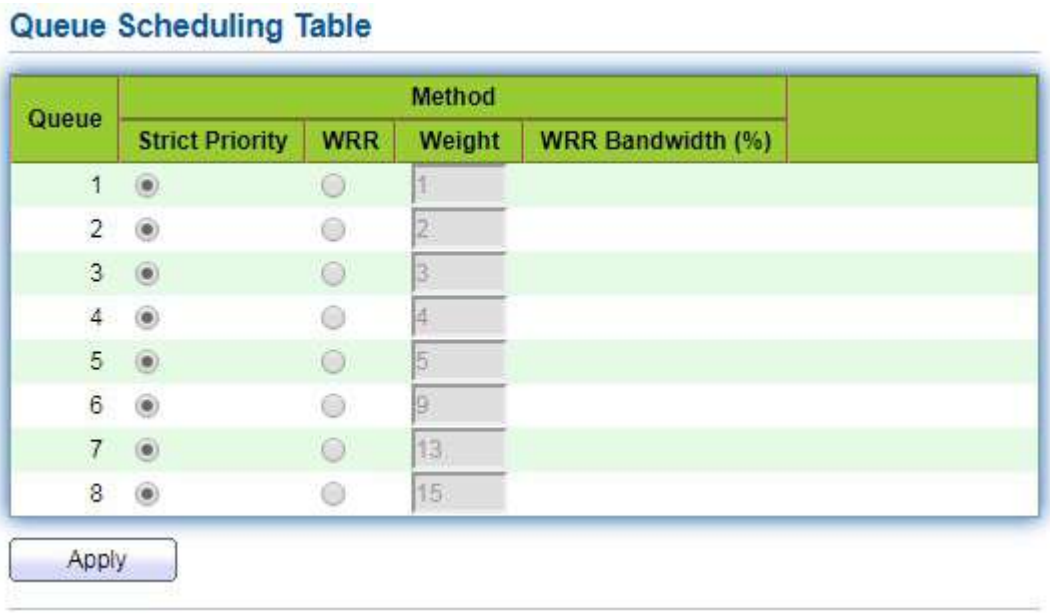
설정 항목	설명
State	글로벌 QoS 기능 전환
Trust Mode	CoS, DSCP, CoS-DSCP 및 IP 우선순위로 나눌 수 있습니다.

포트 구성의 인터페이스 데이터는 다음과 같습니다.

설정 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 우선순위 필드를 표시합니다.

16.1.2 큐 스케줄링

1. “ QoS > 일반 > 대기열 예약”을 클릭합니다. “적용”하고 다음과 같이 마무리합니다.

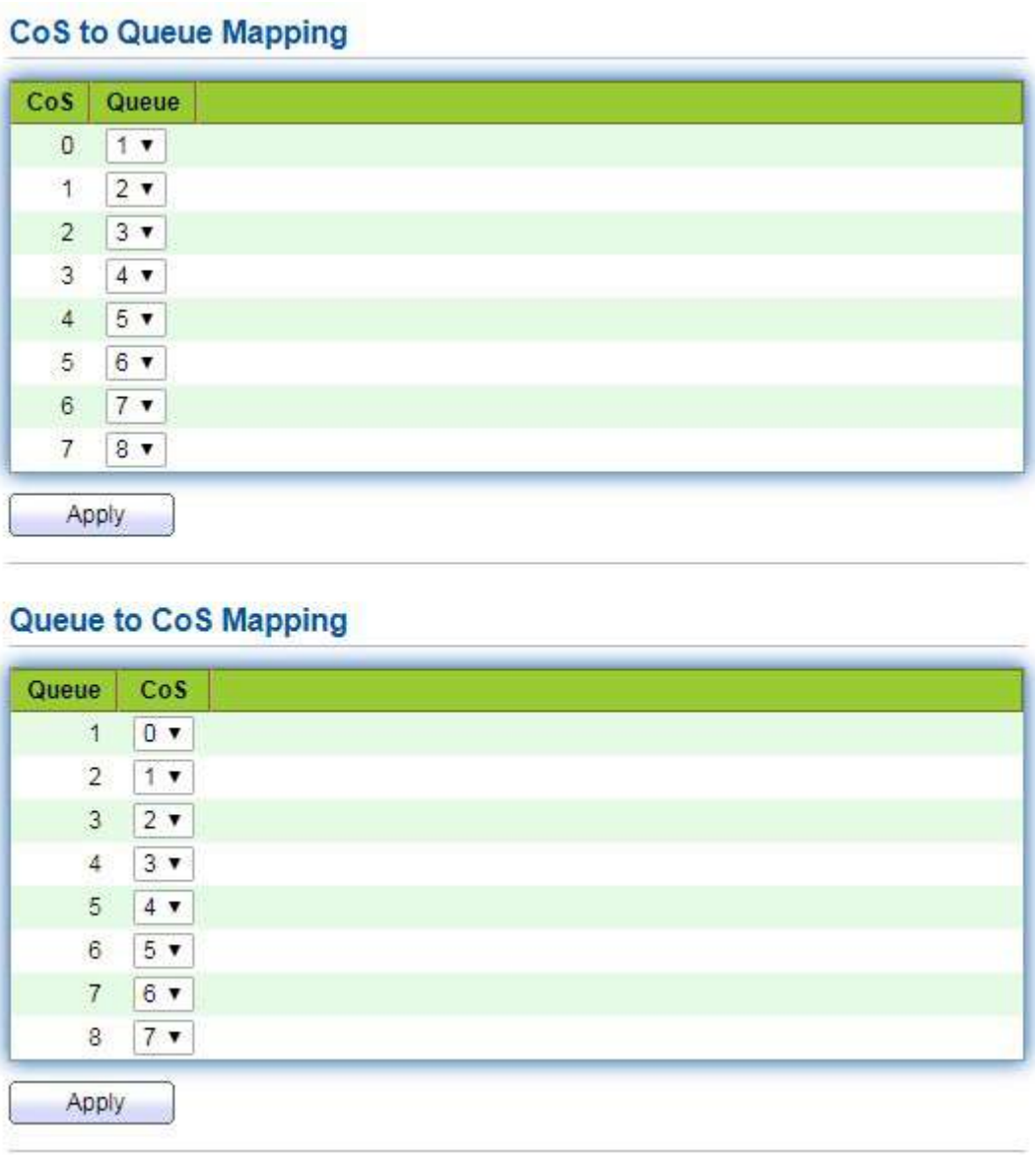


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Strict Priority	SP 모드
WRR	WRR 모드
Weight	대기열이 차지하는 WRR 의 대역폭 비율

16.1.3 CoS 매핑

1. 탐색 표시줄에서 “QoS > 일반 > CoS 매핑”을 클릭합니다. “적용”하고 다음과 같이 마무리합니다.

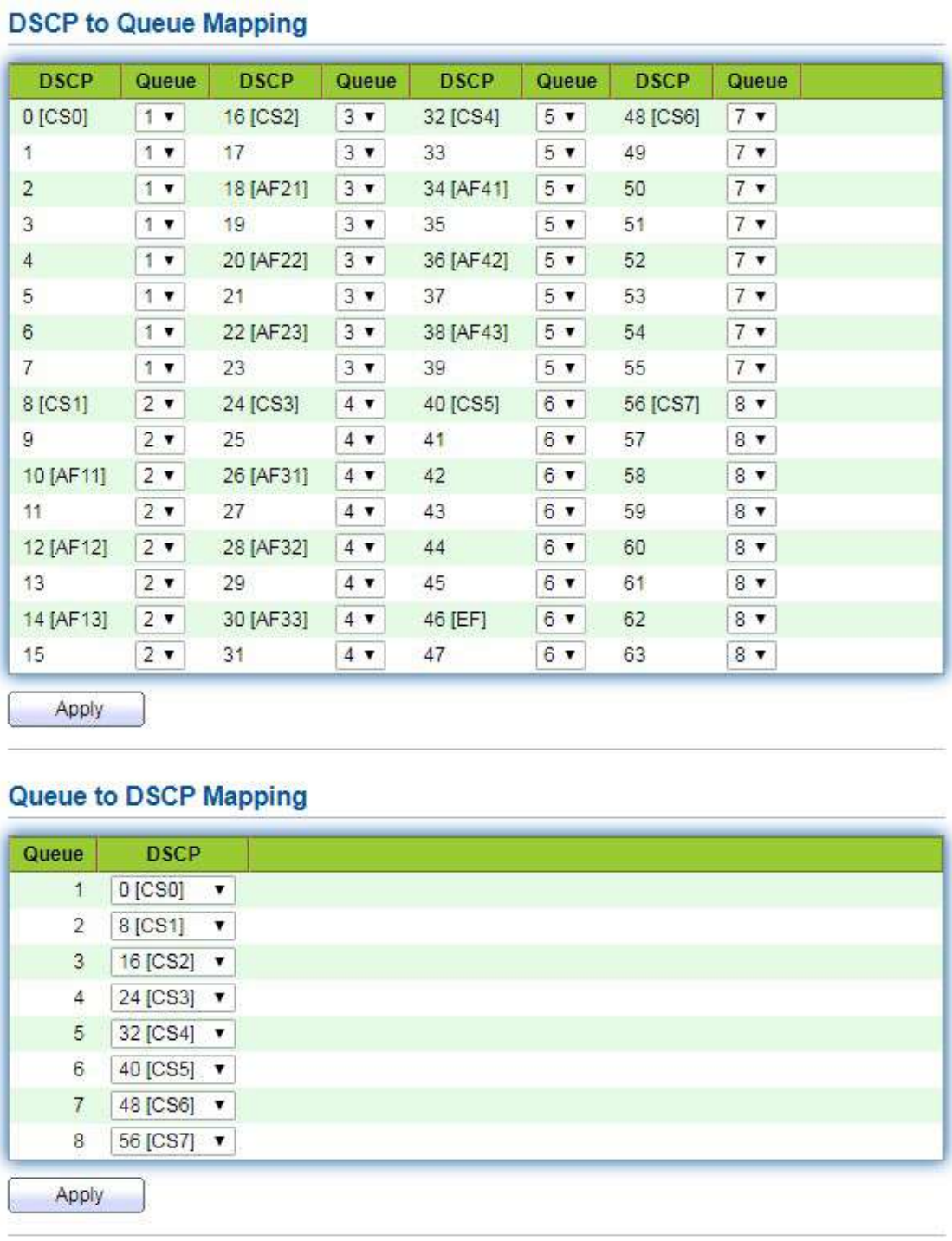


인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
CoS	802.1p 우선순위
Queue	포트 큐

16.1.4 DSCP 매핑

1. “ QoS > 일반 > DSCP 매핑”을 클릭합니다. “적용”하고 다음과 같이 마무리합니다.



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]

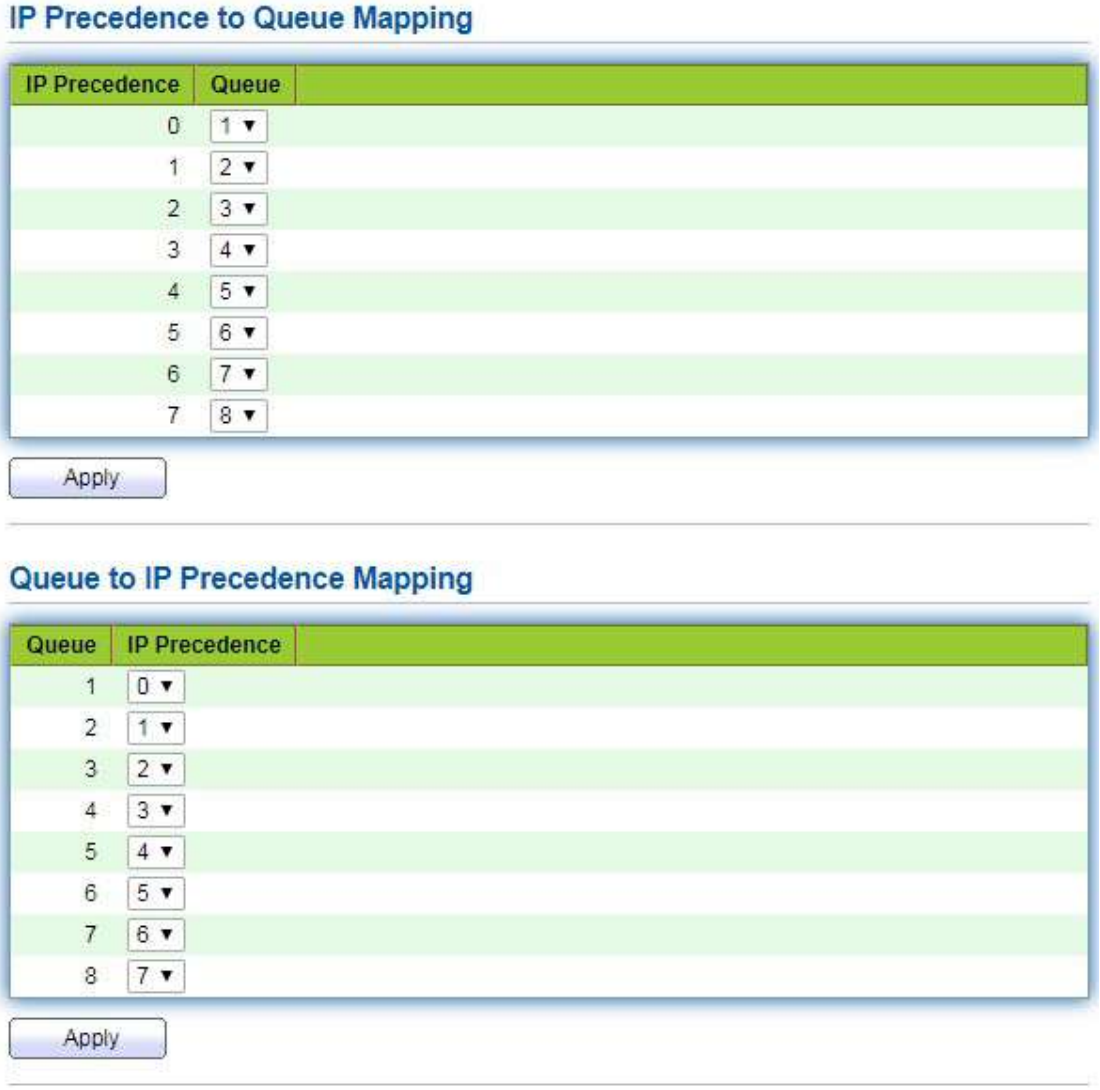
Apply

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
DSCP	IP DHCP 도메인 우선순위 값
Queue	포트 큐

16.1.5 IP 우선순위 매핑

1. “QoS > General > IP Precedence Mapping”을 클릭하고 이 페이지로 진입한 후 “Apply”를 클릭하고 다음과 같이 완료합니다.



인터페이스 데이터는 다음과 같습니다.

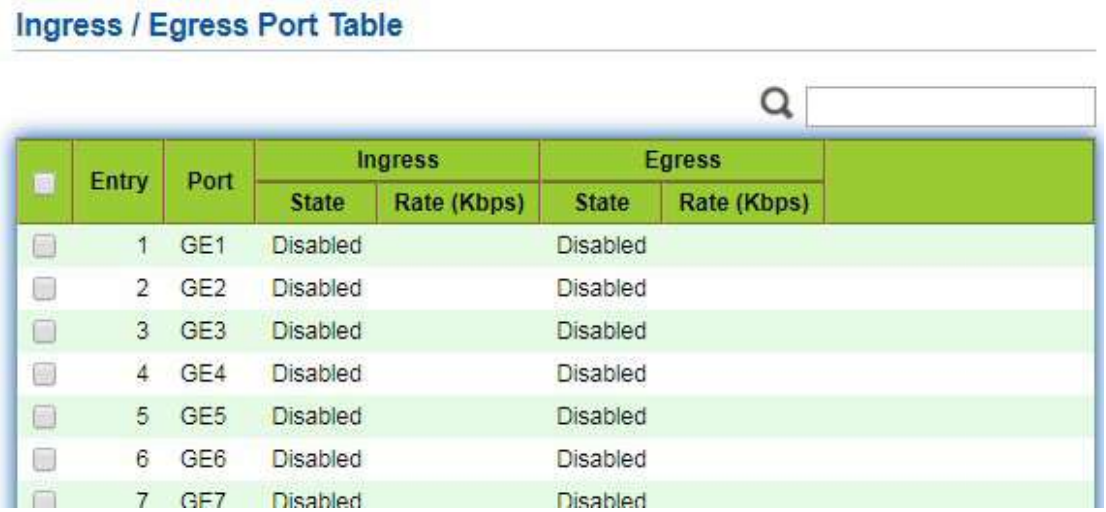
설정 항목	설명
IP Precedence	IP TOS 도메인 우선순위 값
Queue	포트 큐

16.2 Rate limit

16.2.1 Ingress / Egress Port

물리적 인터페이스에서 데이터 전송 및 수신에 대한 속도 제한을 나타냅니다.
흐름을 전송하기 전에 출구에서 속도 제한을 제한하여 나가는 모든 메시지 흐름을 제어합니다.
흐름을 수신하기 전에 수신 시 속도 제한을 제한하여 모든 수신 메시지 흐름을 제어합니다.

1. 탐색 모음에서 “QoS > Rate Limit > Ingress / Egress Port”를 클릭하여 속도 제한 포트를 선택하고 다음과 같이 현재 구성을 확인합니다.



2. 속도 제한을 위한 포트를 선택하고 하단에서 "편집"하여 기능을 전환하고 속도를 지정합니다. "적용"하고 다음과 같이 완료합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명

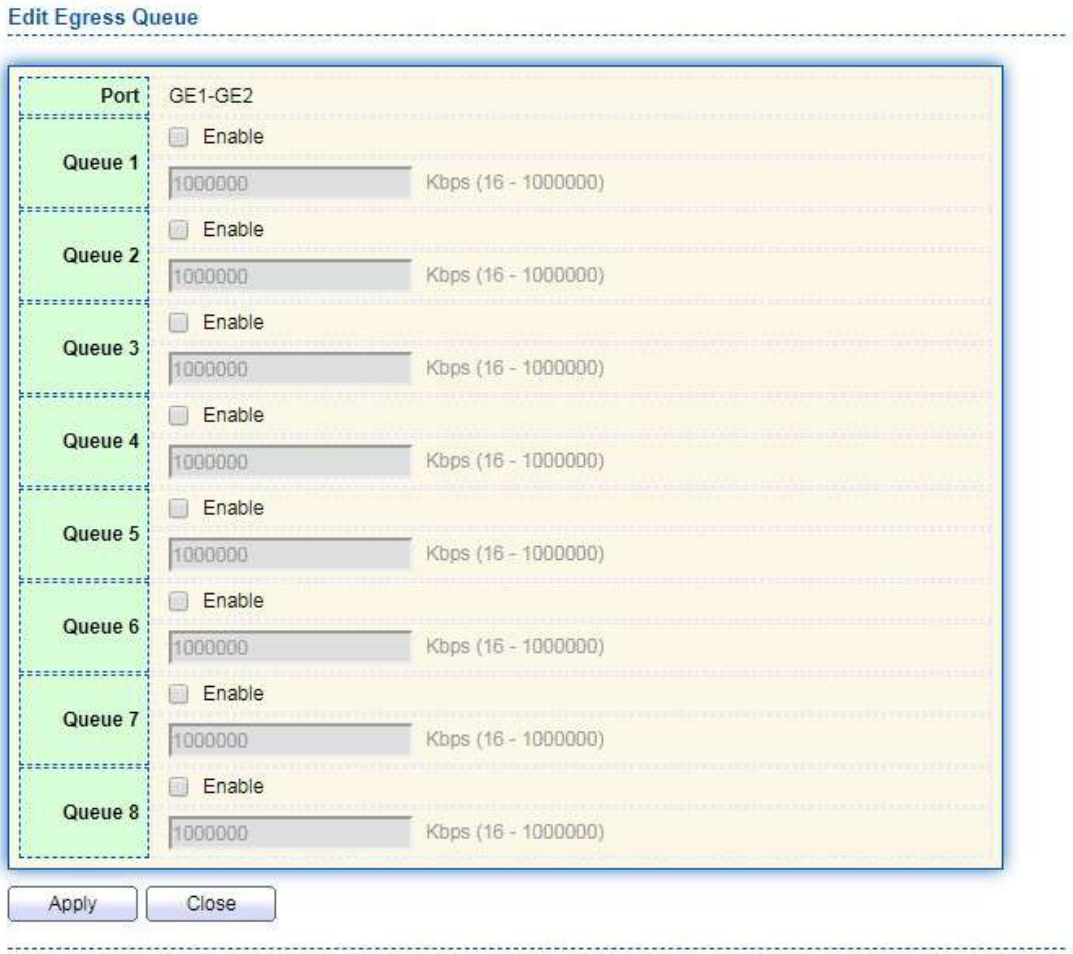
Ingress	Enabled	속도 제한 스위치
	Rate	속도 범위는 16~1,000,000Kbps 입니다.
Egress	Enabled	속도 제한 스위치
	Rate	속도 범위는 16~1,000,000Kbps 입니다.

16.2.2 Egress Queue

송신 대기열 구성 가이드

1. 다음과 같이 네비게이션 바에서 “QoS > Rate Limit > Egress Queue”를 클릭합니다.

2. 포트를 선택하고 "편집"을 클릭하여 다음과 같이 포트 구성 인터페이스로 들어갑니다.

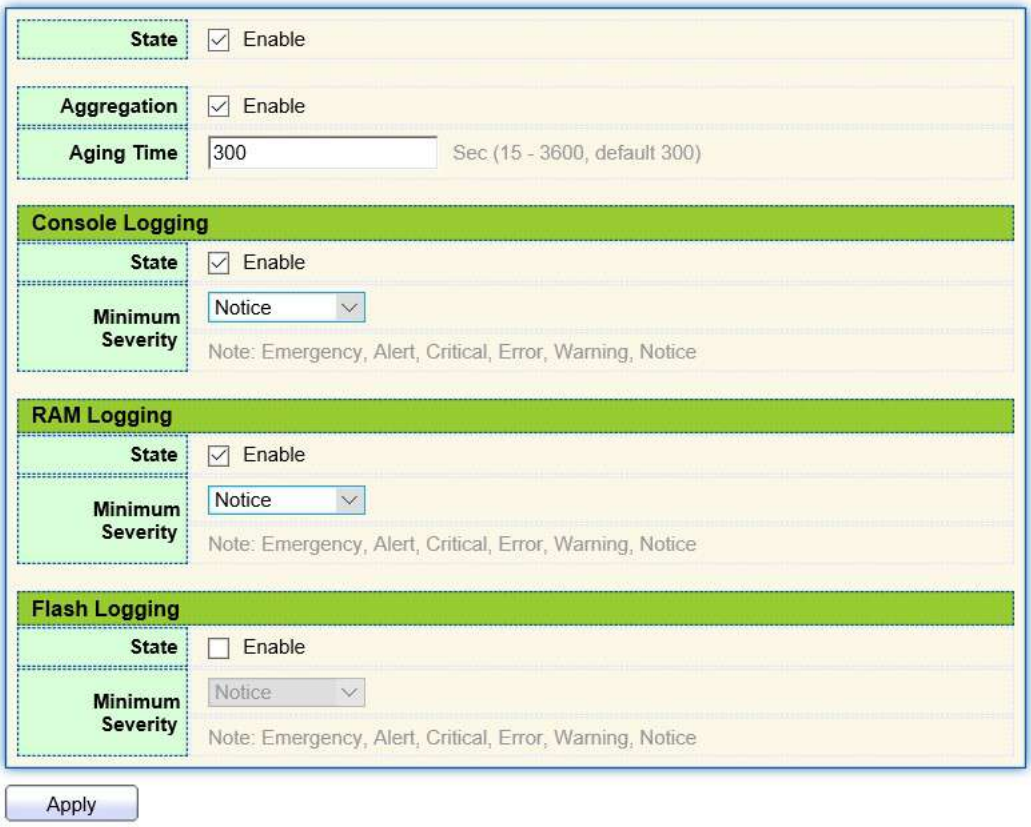


17 진단

17.1 로깅

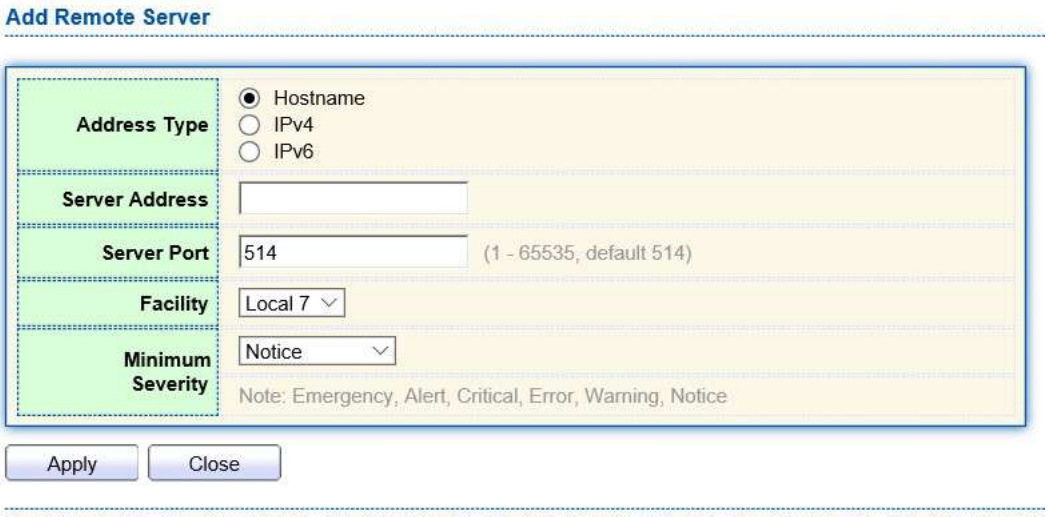
로그 스위치, 정보 통합, 에이징 시간 및 구성 수준을 구성합니다. 또한 스위치의 작업 로그를 TFTP 서버에 업로드합니다.

1. 탐색 모음에서 " Diagnostics > Logging > Property "를 클릭하면 로그 활성화/비활성화, 송신 터미널 선택, 심각도 수준 등을 다음과 같이 구성할 수 있습니다.



2. 탐색 모음에서 " Diagnostics > Logging > Remote Server "를 클릭하여 다음과 같이 서버 구성을 추가하고 확인합니다.

3. “새 원격 로그 서버를 추가하고” 선택한 구성을 “편집”합니다. "적용"하고 다음과 같이 완료합니다.



17.2 Ping

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

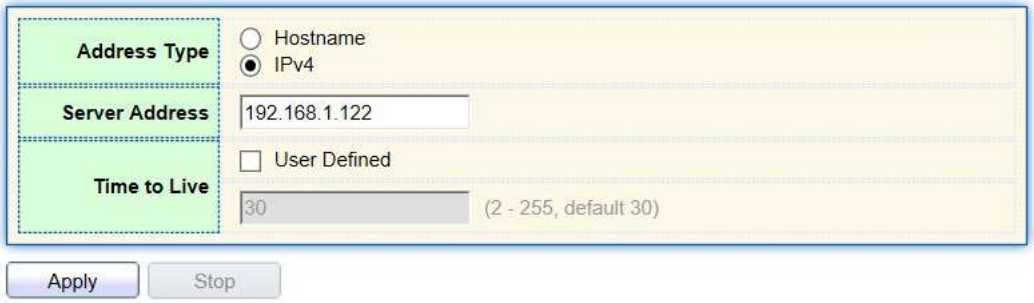
1. 탐색 모음에서 " Diagnostics > Ping "을 클릭하여 다음과 같이 호스트 이름이나 IP 주소 및 테스트 횟수를 입력합니다.

2. “ Ping”을 클릭하여 시스템의 패킷 전송 테스트를 수락하여 주소 유효성을 확인하고 결과를 다음과 같이 출력합니다.

17.3 Traceroute

Traceroute 는 작은 패킷을 전송한 후 대상 장치에서 다시 수신할 때까지의 시간을 측정합니다.

1. 탐색 모음에서 " Diagnostics > Traceroute "를 클릭하여 호스트 이름이나 IP 주소를 입력하여 메시지 존재 시간을 다음과 같이 정의합니다.



2. "Apply"를 눌러 다음과 같이 결과를 테스트하고 출력합니다.

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

구리 테스트는 인그레스 케이블 상태를 평가하고 반사된 전압 강도에 따라 결함 위치(오차로 약 5m)를 찾습니다.

1. 탐색 모음에서 " Diagnostics > Copper Test "를 클릭하여 다음과 같이 테스트할 포트를 선택합니다.

2. “Copper Test”를 클릭하고 다음과 같이 결과를 출력합니다.

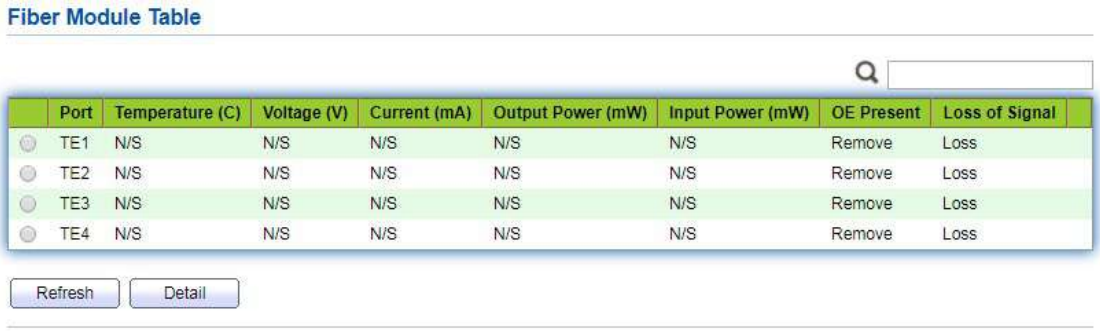
Copper Test Result

Cable Status	
Port	GE1
Result	Open Cable
Length	2.92 M

17.5 Fiber Module

광 모듈 DDM 정보를 보는 데 사용할 수 있습니다.

1. 탐색 모음에서 " Diagnostics > Fiber Module "을 클릭하여 다음과 같이 테스트할 포트를 선택합니다.



17.6 UDLD

UDLD(단방향 링크 감지): 광섬유 또는 연선으로 연결된 이더넷 링크의 물리적 구성을 모니터링하는 데 사용되는 Cisco 개인 레이어-2 프로토콜입니다. 단방향 링크가 나타나면(한 방향으로만 전송할 수 있습니다. 예를 들어 내가 당신에게 데이터를 보낼 수 있고 당신도 그것을 받을 수 있지만 당신이 나에게 보낸 데이터를 받을 수는 없습니다) UDLD 는 이 상황을 감지할 수 있습니다. , 해당 인터페이스를 닫고 경고 메시지를 보냅니다. 단방향 링크는 많은 문제를 일으킬 수 있으며, 특히 루프백을 유발할 수 있는 스패닝 트리 등의 문제가 발생할 수 있습니다. 참고: 정상적으로 실행하려면 링크 양쪽 끝에 있는 장치에서 UDLD 를 지원해야 합니다.

17.6.1 프로퍼티

글로벌 및 포트 스위치 구성

1. 탐색 바에서 “Diagnostics > UDLD > Property ”를 클릭하여 다음과 같이 테스트할 포트를 선택합니다.

2. 포트를 선택하고 "편집"을 클릭하여 다음과 같이 편집 인터페이스로 들어갑니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Port	포트 ID
Mode	UDLD 포트 모드 Disabled: 포트 기능 비활성화 Normal: UDLD 는 단방향 링크를 감지하고 포트를 미확인으로 표시하여 시스템 로그를 생성할 수 있습니다. Aggressive: UDLD 는 단방향 링크를 감지할 수 있습니다. 링크 재구축을 시도하고 8 초 동안 계속해서 UDLD 메시지를 보냅니다. UDLD 에코 응답이 없으면 포트는 오류 가능 상태가 됩니다.

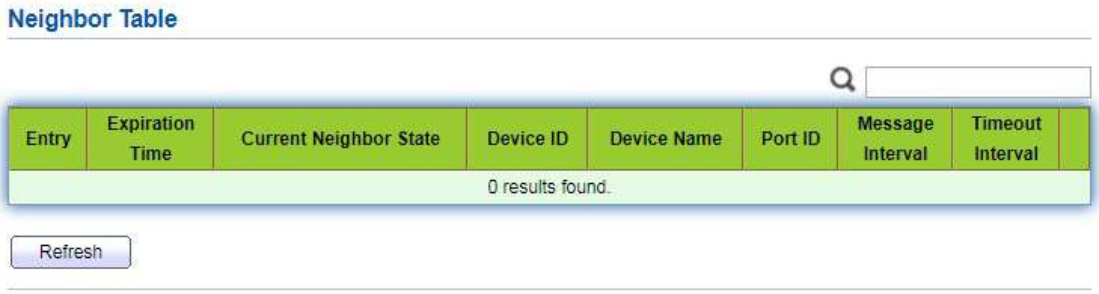
17.6.2 Neighbor

UDLD 는 각 활성 인터페이스에서 주기적으로 hello 패킷(광고 또는 프로브 프로브라고도 함)을 보냅니다.

스위치가 Hello 패킷을 수신하면 메시지는 에이징 시간이 만료될 때까지 저장됩니다. 에이징 시간이 만료되기 전에 Hello 를 다시 수신하면 에이징 시간이 새로 고쳐집니다.

새로운 이웃이나 이웃이 캐시 재동기화를 요청하면 일련의 UDLD 프로브/에코(Hello) 패킷이 전송됩니다.

1. 탐색 표시줄에서 " Diagnostics > UDLD > Neighbor "을 클릭하여 다음과 같이 테스트할 포트를 선택합니다.



인터페이스 데이터는 다음과 같습니다.

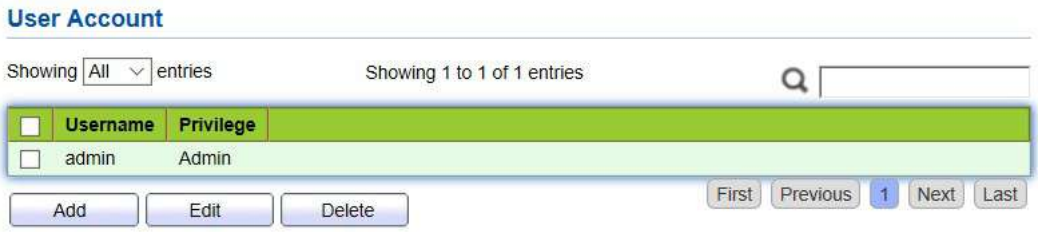
설정 항목	설명
Entry	이웃 일련번호
Expiration Time	남은 에이징 시간
Current Neighbor State	이웃현황
Device ID	이웃의 장치 ID
Device Name	이웃의 장치 이름
Port ID	연결된 인터페이스의 ID
Message Interval	이웃을 위한 메시지 간격
Timeout Interval	이웃에 대한 시간 초과 간격

18 관리

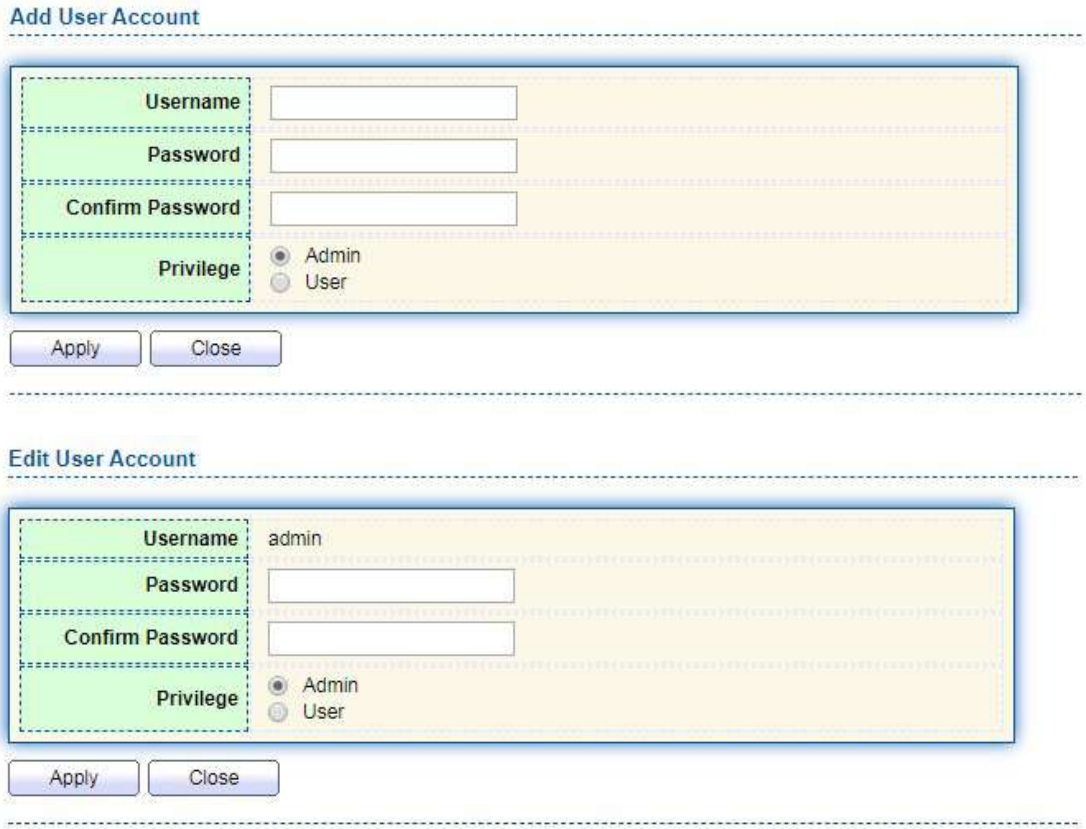
18.1 사용자 계정

사용자는 스위치의 현재 사용자 이름, 비밀번호, 권한을 확인하고 수정할 수 있습니다.

1. 네비게이션 바에서 “Management > User Account”을 클릭하면 다음과 같이 기본적으로 “admin” 사용자 이름과 “Admin” 권한을 확인할 수 있습니다.



2. 다음과 같이 새 사용자 계정을 "추가"하고 선택한 사용자 속성을 "편집"합니다.



18.2 펌웨어

시스템 버전 펌웨어 업그레이드

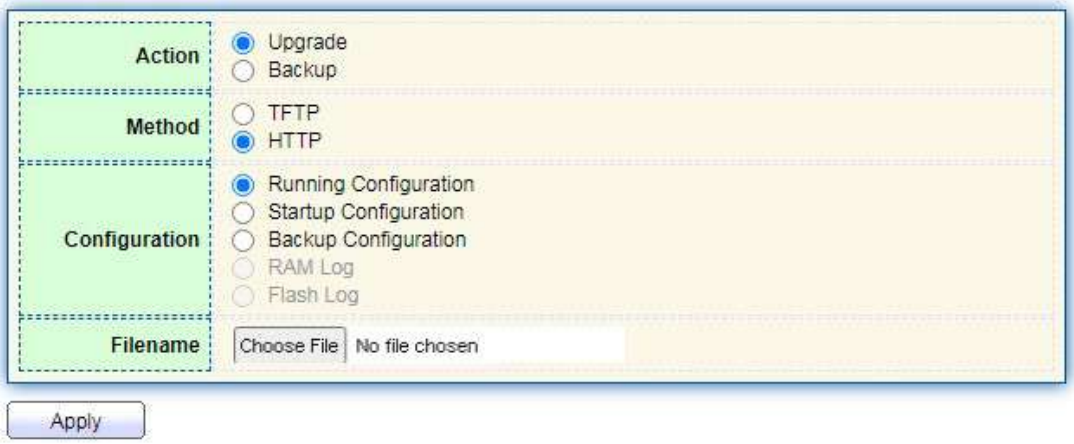
1. 다음과 같이 탐색 표시줄에서 “Management > Firmware > Upgrade ”를 클릭합니다.

18.3 환경 설정

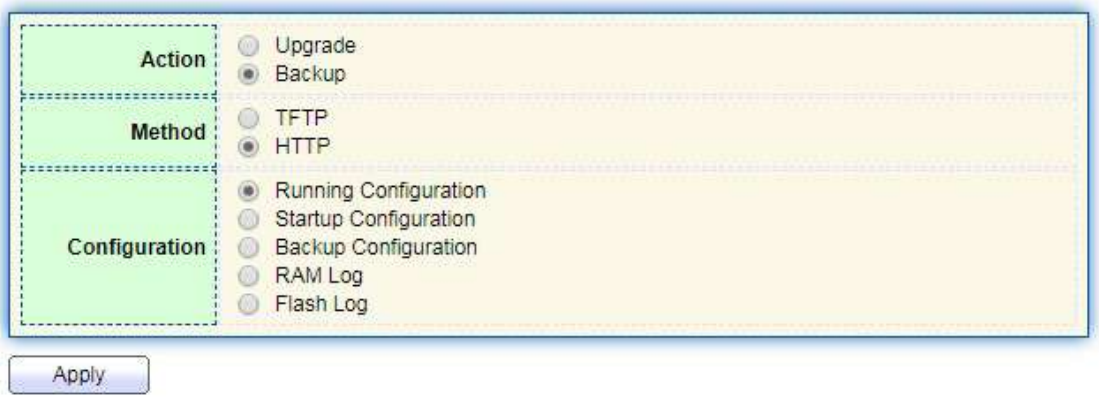
18.3.1 업그레이드

시스템 구성 업그레이드 또는 백업

1. " Management > Configuration > Upgrade "를 클릭하고 "TFTP" 또는 "HTTP" 모드에서 "업그레이드"를 클릭하고 업그레이드할 해당 파일을 선택합니다(서버는 TFTP 모드로 표시되어야 함). "적용"하고 다음과 같이 완료합니다.



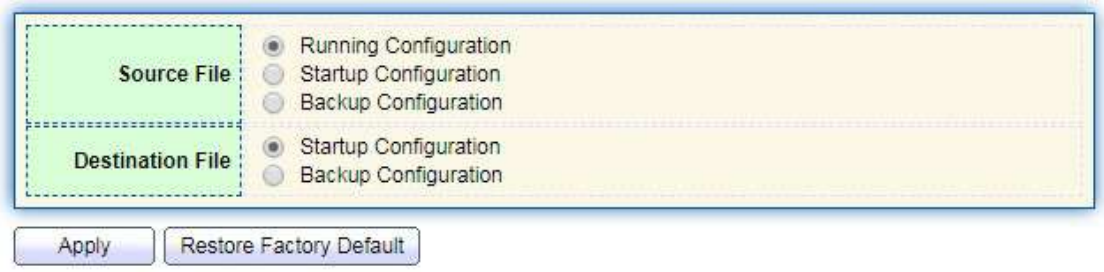
2. "TFTP" 또는 "HTTP" 모드에서 "백업"을 클릭하고 업그레이드할 파일이나 로그를 선택합니다(서버는 TFTP 모드로 표시되어야 함). “적용”하고 다음과 같이 마무리합니다.



18.3.2 환경 설정 저장

시스템 구성을 저장하거나 구성을 공장 기본값으로 복원

1. 다음과 같이 탐색 모음에서 " Management > Configuration > Save Configuration "을 클릭합니다.

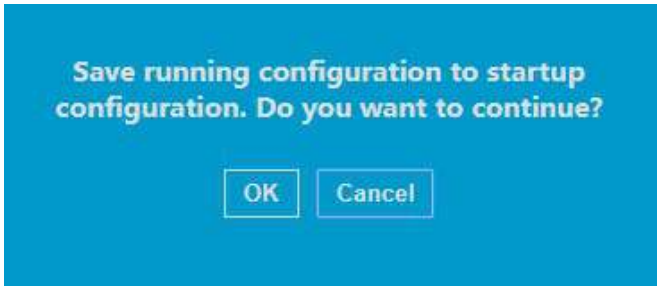


Note:

● 공장 설정을 복원하려면 "공장 초기화" 및 "장치 다시 시작"을 클릭하세요. "실행 구성"을 "시작 구성"("백업 구성" 또는 "실행 구성"으로 저장 가능) 및 "백업 구성"("시작 구성" 또는 "실행 구성"으로 저장 가능)으로 저장합니다.).

:

2. 오른쪽 상단의 “Save”를 클릭하면 아래와 같이 실행 중인 구성이 시작 구성으로 저장됩니다.

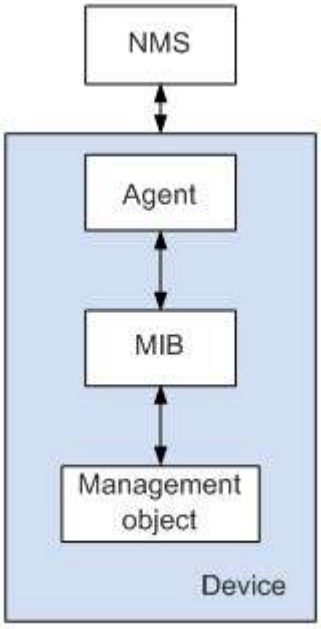


18.4 SNMP

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

- Simple: 폴링 구동 SNMP 는 빠른 속도와 저렴한 비용으로 소규모 환경에 적용할 수 있는 기본 기능 세트를 갖추고 있습니다. 게다가 UDP 기반 SNMP 는 대부분의 장치와 호환됩니다. 강력함: SNMP 는 관리자가 정보를 쉽게 검색, 수정 및 문제 해결할 수 있도록 두 노드 간의 관리 정보 전송을 보장하는 것을 목표로 합니다. SNMPv1, v2c 및 v3 의 3 가지 일반적인 버전이 있습니다. 해당 시스템에는 NMS(네트워크 관리 시스템), 에이전트, 관리 개체 및 MIB(관리 정보 베이스)가 포함되어 있습니다.
- NMS, 관리 센터로서 모든 기기를 관리하게 됩니다. 관리 중인 각 장치에는 상주 에이전트, MIB 및 관리 개체가 포함됩니다. NMS 는 NMS 명령을 실행하기 위해 MIB 를 작동하는 관리 개체에서 실행되는 에이전트와 상호 작용합니다.

SNMP 관리 모델



NMS

- NMS 는 네트워크 관리자로서 자신의 서버에서 SNMP 를 통해 네트워크 장비를 관리/모니터링합니다. 지정된 매개변수를 조회하거나 수정하도록 에이전트에 요청할 수 있습니다. NMS 는 에이전트가 적극적으로 전송한 트랩을 수신하여 관리 장치의 상태를 업데이트할 수 있습니다.

Agent

- 관리되는 장치의 에이전트 프로세스로 장치 데이터를 유지하고, 관리 데이터를 보고하여 NMS 요청에 응답합니다. 에이전트는 MIB 테이블을 통해 관련 주문을 이행하고 요청을 받은 후 결과를 NMS 로 다시 전송합니다. 장애나 다른 이벤트가 발생하면 장치는 에이전트를 통해 장치의 현재 상태와 관련된 정보를 주도적으로 NMS 로 전송합니다.

Management object

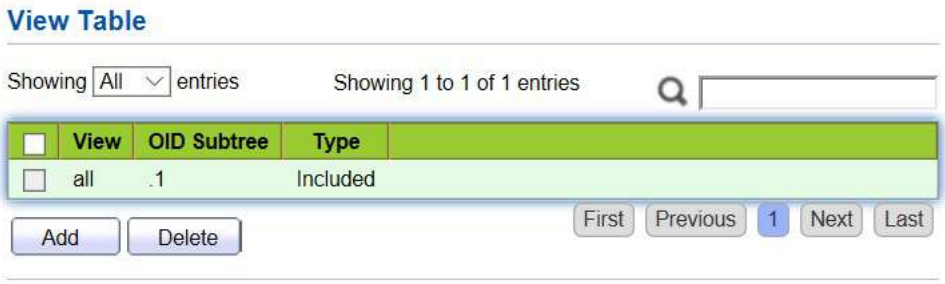
- 관리 중인 개체를 말합니다. 각 장치에는 하드웨어(예: 인터페이스 보드), 부분 하드웨어 및 소프트웨어(예: 라우팅 프로토콜), 기타 구성 항목 세트를 포함하여 둘 이상의 개체가 있을 수 있습니다.

MIB

- MIB 는 관리 객체가 유지하는 변수(즉, Agent 가 조회하고 설정할 수 있는 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 설정 항목을 설정합니다.

18.4.1 보기

1. 다음과 같이 탐색 표시줄에서 “Management > SNMP > View”를 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
View	이름 보기
OID Subtree	OID 보기
Type	보기 유형:'포함됨' 또는 '제외됨'

2. “추가” 해당 구성을 “적용”하고 완료합니다.

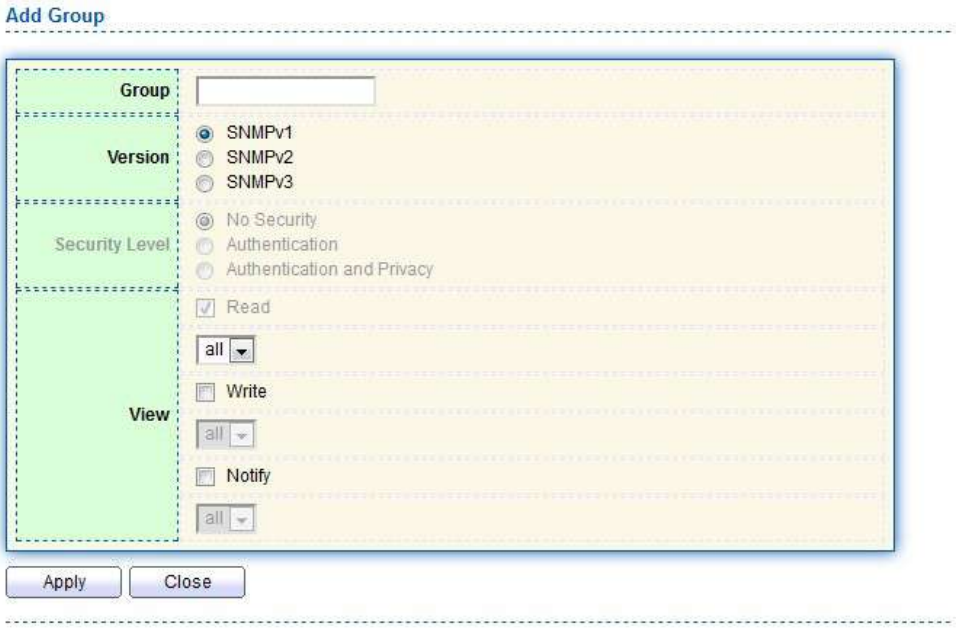
18.4.2 그룹

1. 다음과 같이 탐색 표시줄에서 “Management > SNMP > Group”을 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Group	그룹 이름
Version	V1, V2, V3
Security Level	보안 수준
View	뷰는 뷰 읽기, 쓰기, 알림으로 구분됩니다.

2. 해당 구성을 작성하려면 "추가"를 클릭하십시오. "적용"하고 마무리합니다.



18.4.3 커뮤니티

1. 다음과 같이 탐색 표시줄에서 “Management > SNMP > Community ”를 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Community	커뮤니티 구성
Group	그룹 이름
View	이름 보기
Access:	권한: 읽기 전용 또는 읽기-쓰기

2. 해당 구성을 "추가"합니다. "적용"하고 마무리합니다.

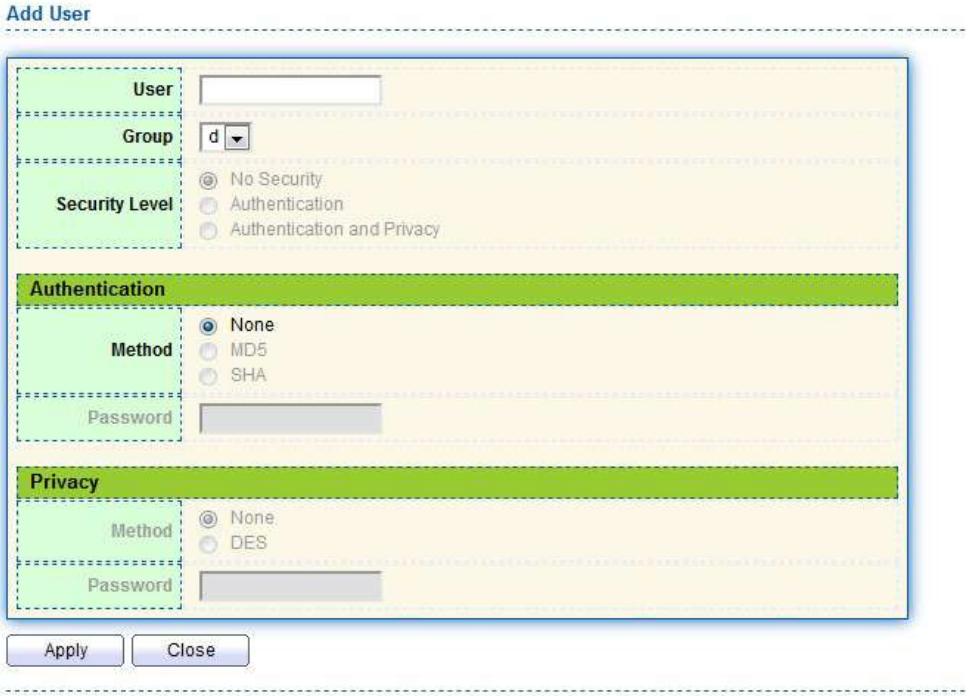
18.4.4 유저

1. 다음과 같이 탐색 표시줄에서 “Management > SNMP > User”를 클릭합니다.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
User	사용자 이름
Group	그룹 이름
Security Level	보안 수준
Authentication Method	인증 모드
Privacy Method	암호화 모드

2. 해당 구성을 "추가"합니다. "적용"하고 마무리합니다.



18.4.5 Engine ID

1. 다음과 같이 네비게이션 바에서 “Management > SNMP > Engine ID”를 클릭하세요.

2. “사용자 자동화”를 클릭하여 해당 ID 값을 입력하세요. "적용"하고 마무리합니다.

18.4.6 트랩 이벤트

1. 다음과 같이 네비게이션 바에서 “Management > SNMP > Trap Event ”를 클릭하세요.

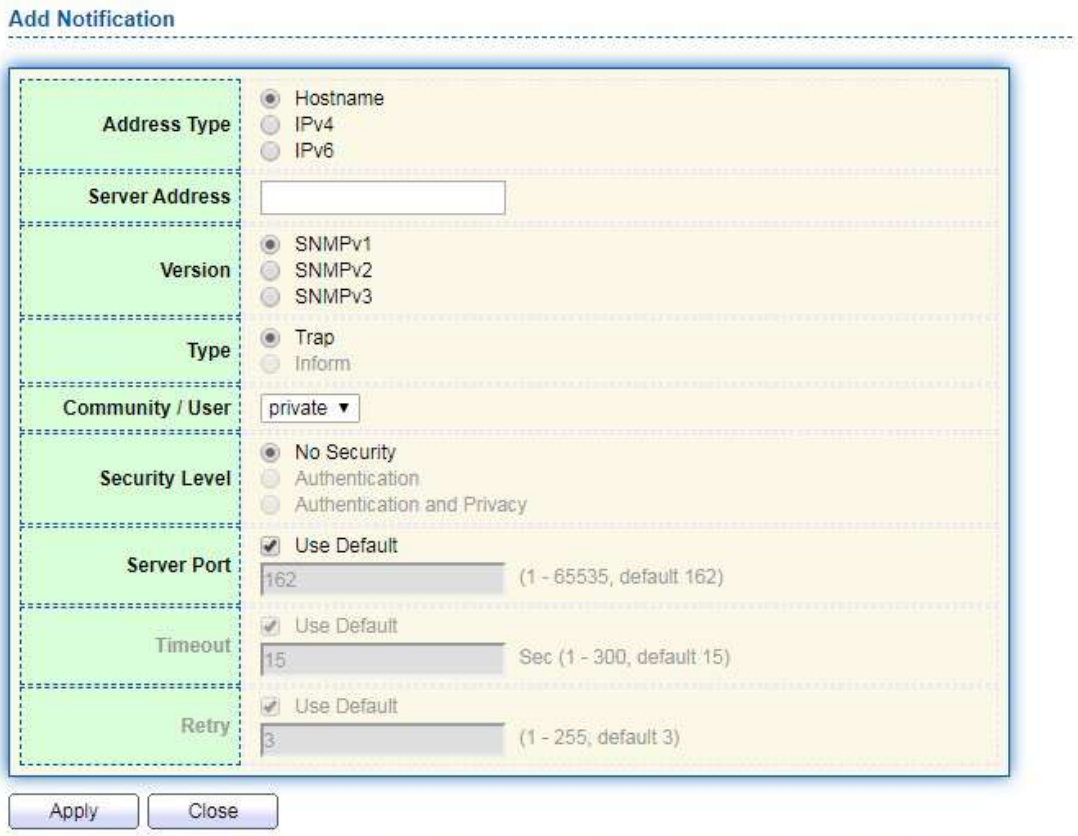
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Authentication Failure	인증 오류
Link Up / Down	포트 링크 업/다운
Cold start	콜드 스타트
Warm start	따뜻한 시작

2. ““적용”하고 마무리합니다.

18.4.7 Notification

1. 다음과 같이 탐색 표시줄에서 “Management > SNMP > Notification ”을 클릭합니다.



인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Address Type	주소 유형: "호스트 이름", "IPv4" 또는 "IPv6"
Server Address	서버 주소 정보
Version	SNMP 버전: v1, v2 및 v3
Type	알림 유형: "트랩" 또는 "알림"
Community / User	커뮤니티 또는 사용자 이름
Security Level	보안 수준
Server port	기본적으로 162(1~65,535 범위)
Timeout	시간 초과 기간: 기본적으로 15 초(1~300 초 범위).
Retry	재시도 간격 범위는 1~255 초이며 기본적으로 3 초입니다.

2. 해당 구성을 "추가"합니다. "적용"하고 마무리합니다.

18.5 RMON

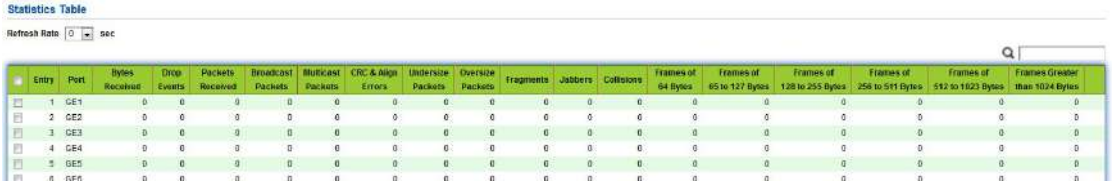
RMON(Remote Monitoring)은 IETF(Internet Engineering Task Force)에서 정의한 MIB 로 MIB II 표준을 크게 강조합니다. 널리 사용되는 네트워크 관리 표준 중

하나인 네트워크 세그먼트 또는 전체 네트워크의 데이터 흐름을 주로 모니터링합니다. RMON 에는 NMS(Network Management Station)와 다양한 네트워크 장치에서 실행되는 에이전트가 포함되어 있습니다. 네트워크 모니터 또는 탐지기에서 실행되는 RMON 에이전트는 포트에 연결된 네트워크 세그먼트의 흐름 정보(예: 특정 기간 동안 네트워크 세그먼트의 총 메시지 수 또는 호스트로 전송된 올바른 메시지의 수)를 추적하고 계산합니다. . SNMP 아키텍처를 기반으로 하는 RMON 은 기존 SNMP 프레임워크와 호환됩니다. SNMP 는 보다 효율적이고 적극적인 방식으로 원격 네트워크 장치를 모니터링하여 서브넷 작동을 감독합니다. RMON 은 NMS 와 SNMP Agent 간의 통신 흐름을 줄여 대규모 상호 연결 네트워크를 편리하고 효과적으로 관리할 수 있습니다. 다중 모니터는 2 가지 방법으로 데이터를 수집할 수 있습니다. 전용 RMON 프로브를 사용하여 데이터를 수집하고, NMS 가 직접 정보를 관리하고 네트워크 리소스를 제어합니다. 모든 RMON MIB 정보를 얻을 수 있습니다. 네트워크 장치(라우터, 스위치, HUB 등)에 직접 접근할 수 있는 RMON 에이전트는 RMON 프로브 기능을 갖춘 네트워크 시설이 됩니다. RMON NMS 는 SNMP 기본 명령으로 SNMP Agent 와 데이터를 교환하여 네트워크 관리 정보를 수집합니다. 그러나 장치 리소스의 제한으로 인해 일반적으로 RMON MIB 의 모든 데이터를 가져오지 못합니다. 대부분의 장치는 알람, 이벤트, 기록 및 통계 그룹의 네 가지 그룹에서만 데이터를 수집합니다. Area 형 스위치는 두 번째 방식으로 RMON 을 구현합니다. 스위치에 직접 접근하는 RMON Agent 는 RMON 프로브 기능을 갖춘 네트워크 설비가 됩니다. 스위치가 지원하는 SNMP Agent 를 실행함으로써 NMS 는 네트워크 관리를 위해 포트에 연결된 네트워크 세그먼트에 대한 전체 흐름, 오류 통계, 성능 통계 및 기타 정보를 얻을 수 있습니다.

18.5.1 통계

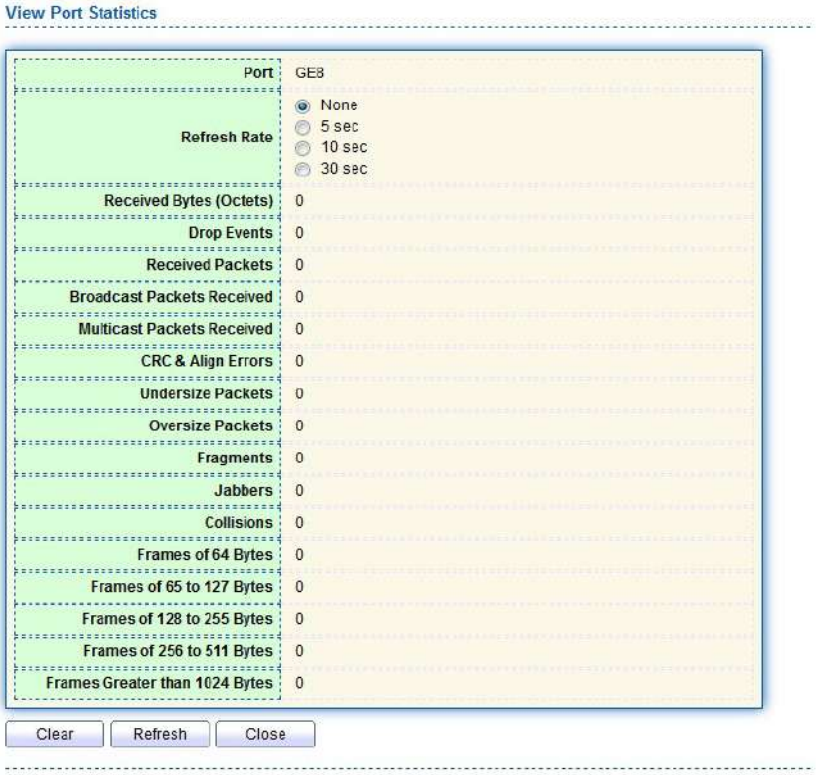
통계 그룹 정보는 스위치의 각 모니터링 인터페이스에 대한 통계, 즉 그룹 생성 초기부터 누적된 정보를 반영합니다. 통계에는 네트워크 충돌 횟수, CRC 오류 메시지, 너무 작은(너무 큰) 데이터 메시지, 브로드캐스트/멀티캐스트 메시지, 수신된 바이트 및 메시지 등이 포함됩니다. RMON 통계 및 관리 기능을 통해 포트 사용 및 발생한 오류를 확인할 수 있습니다. 각각 모니터링하고 계산했습니다.

1. 다음과 같이 탐색 표시줄에서 “Management > RMON > Statistics”를 클릭하면 포트 관련 메시지 통계가 표시됩니다.



2. 선택한 포트의 통계를 "지우기" 및 "새로 고침"합니다. 다음과 같은 통계를

"보기"합니다.



3. 자동으로 작동하려면 지정된 새로 고침 빈도를 선택하십시오.

18.5.2 History

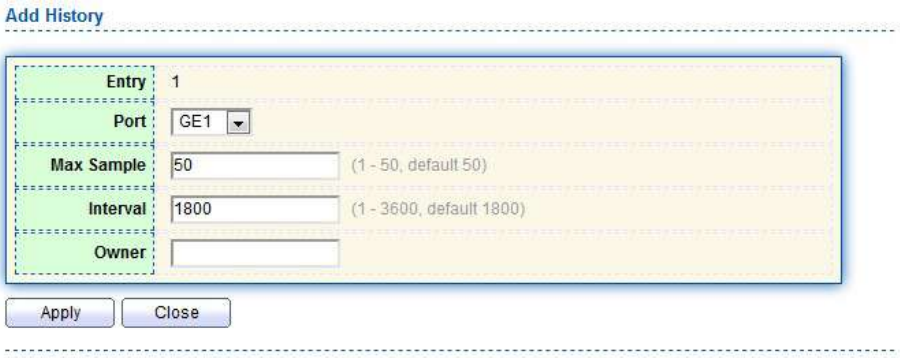
RMON 기록 그룹을 구성하면 스위치는 간편한 처리를 위해 정기적으로 네트워크 통계를 수집하고 임시 저장하여 네트워크 세그먼트 흐름, 오류 패킷, 브로드캐스트 패킷, 대역폭 활용도 및 기타 통계에 대한 기록 데이터를 제공합니다. 이력 데이터 관리는 특정 포트의 데이터에 대한 정기적인 수집 및 유지 관리를 포함하여 이력 데이터 수집 측면에서 장치를 설정하는 데 사용할 수 있습니다.

1. 다음과 같이 네비게이션 바에서 “Management > RMON > History ” 을 클릭하세요.

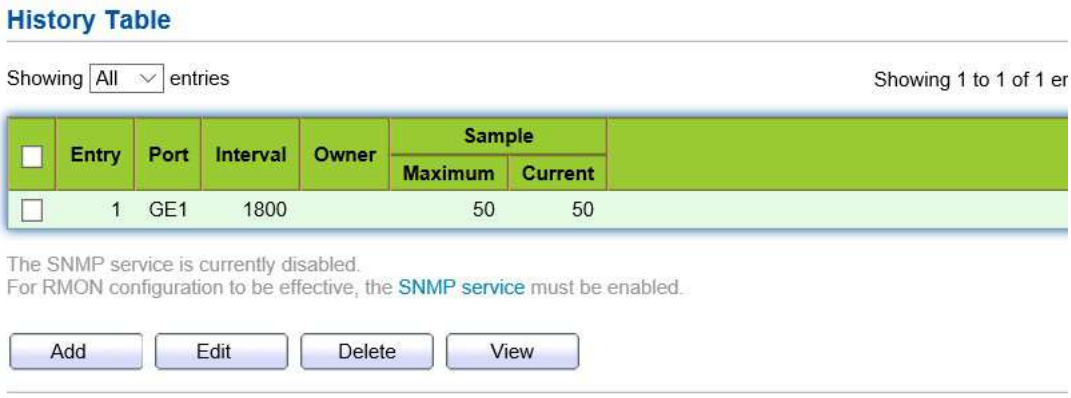
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Entry	이벤트 그룹 일련번호
Port	계산할 포트
Interval	샘플링 간격 범위는 1~3,600(단위: s)이며 기본적으로 1,800 초입니다.
Owner	소유자
Maximum	최대 샘플 수의 범위는 0~50 이며 기본적으로 50 입니다.
Current	현재 샘플 수

2. 기록 그룹을 구성하려면 해당 구성 항목을 “추가”하세요.



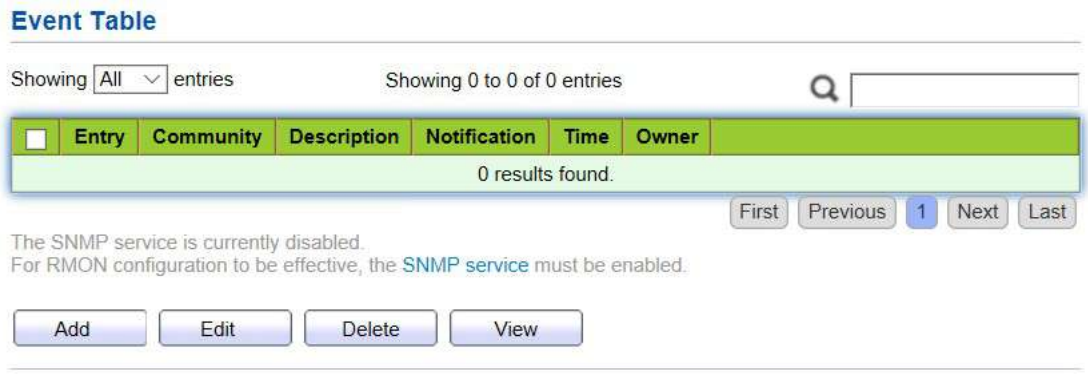
3. “적용”을 선택하고 다음과 같이 마무리합니다.



18.5.3 Event

이벤트 번호 및 처리 방식을 정의하는 이벤트 그룹은 주로 경보 그룹 설정 항목과 확장 경보 그룹 설정 항목에 의해 발생되는 이벤트에 대한 것입니다. 이에 대한 몇 가지 해결 방법이 있습니다: 로그 테이블에 기록; Trap 메시지를 NMS 로 전송하는 단계; 로그를 기록하고 Trap 메시지를 전송하는 단계;

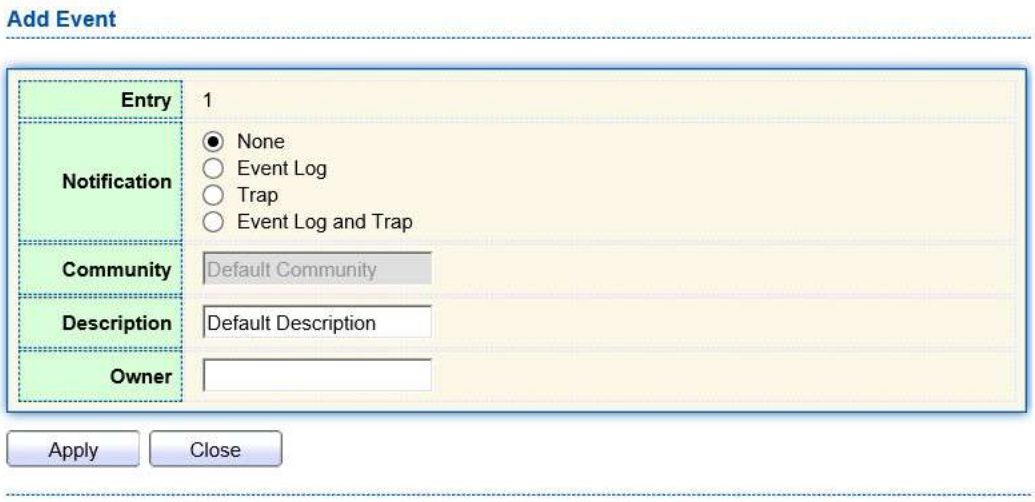
1. 아래와 같이 네비게이션 바에서 “Management > RMON > Event ” 를 클릭하세요.



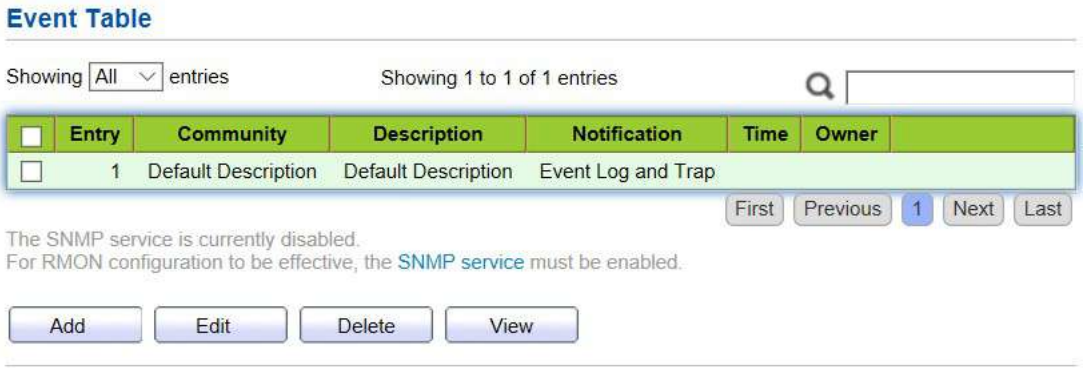
인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Entry	이벤트 그룹 일련번호
Community	커뮤니티 이름
Description	설명
Notification	공고
Timer	시간
Owner	소유자

2. “이벤트 그룹을 구성하려면 해당 구성 항목을 "추가"하십시오.



3. "추가"하고 다음과 같이 마무리합니다.



18.5.4 Alarm

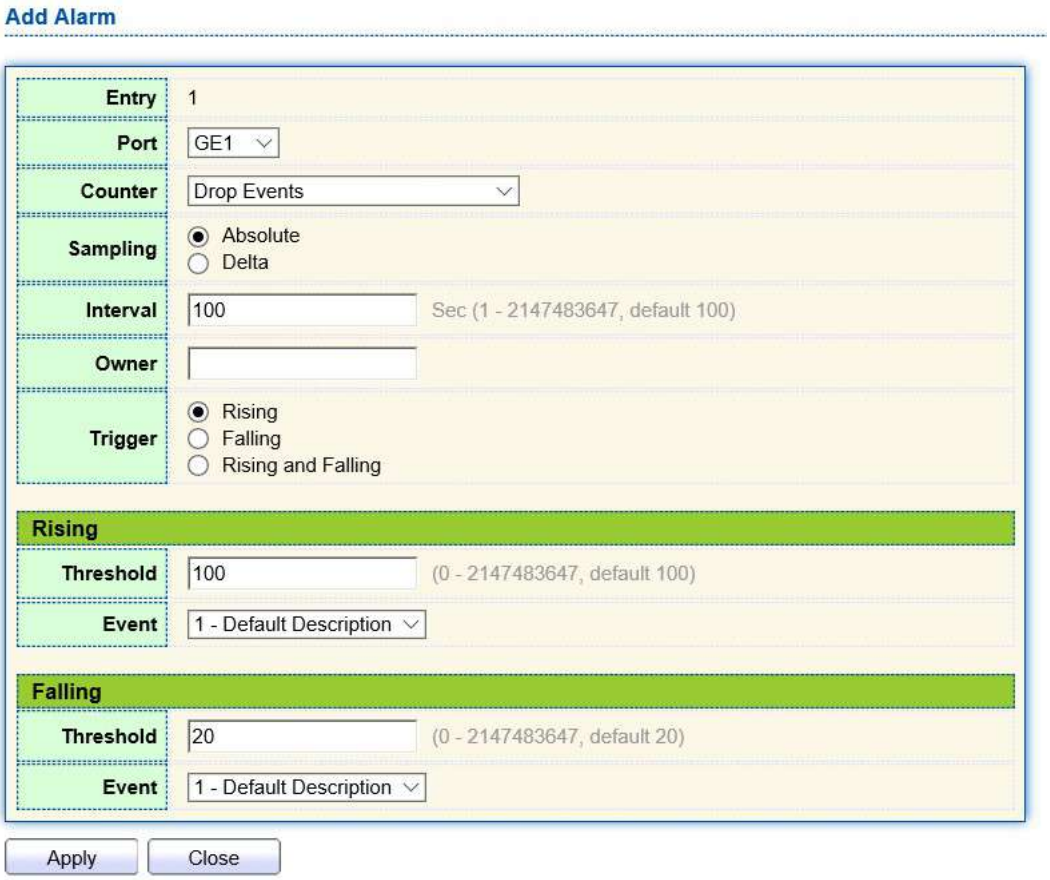
RMON 경보 관리는 포트 통계와 같은 특정 경보 변수를 모니터링합니다. 모니터링된 데이터의 값이 해당 방향으로 정의된 임계값을 초과하는 경우 알람 이벤트가 발생하며, 이는 처방된 치료 모드에 따라 처리됩니다. 이벤트 정의는 이벤트 그룹에서 구현됩니다. 사용자가 알람 항목을 정의한 후 시스템은 다음과 같이 처리합니다. 샘플링 시간으로 정의된 알람 변수를 샘플링하고 값을 임계값과 비교해야 합니다. 임계값이 높을수록 해당 이벤트가 트리거됩니다.

1. 다음과 같이 네비게이션 바에서 “Management > RMON > Alarm”을 클릭하세요.

인터페이스 데이터는 다음과 같습니다.

설정 항목	설명
Entry	경보그룹 일련번호
Port	계산할 포트를 입력하세요.
Counter	알람의 샘플 매개변수
Interval	샘플링 간격의 범위는 1 부터 2,147,483,647 까지이며 단위는 초입니다. 기본적으로 100 초입니다.
Sampling	샘플 유형: 절대 및 삭제
Owner	소유자
Threshold (Rising)	상승 에지의 임계값 범위는 0 부터 2,147,483,647 까지입니다.
Event (Rising)	이벤트 그룹 인덱스. 알람이 발생하면 해당 이벤트가 활성화됩니다.
Threshold (Falling)	하강 에지의 임계값 범위는 0 부터 21,474,836,475 까지입니다.
Event (Falling)	이벤트 그룹 인덱스. 알람이 발생하면 해당 이벤트가 활성화됩니다.

2. 알람 그룹을 구성하려면 해당 구성 항목을 추가하십시오.



3. “적용”을 선택하고 다음과 같이 마무리합니다.