사 용 자 메 뉴 얼

MV-SERIES

통합 메뉴얼

MIRAE SIGNAL

www.miraesignal.com

개정 이력

일자	주요개정 내용	문서 버전
2024-07-03	초판	V_1.0
2024-11-22	2.12 ARP Information 수정 및 추가 3.1.2.1 Creating VLAN 수정 및 추가 3.2.3 Port Mirroring 수정 및 추가 3.4 ERPS 4.2.2 IGMP Snooping 설정 및 추가 5.6 Syslog Server 내용 추가	V_1.1

-목 차-

1. WEB OVERVIEW 8
_1.1 개요 8
_1.2 웹 접속 방법 9
_1.3 웹에서 로그아웃 10
_1.4 설정 저장 11
_1.5 REBOOT 12
_1.6 웹 인터페이스 13
_1.7 웹 기반 기능 소개 14
2. MONITOR 16
_2.1 개요 16
_2.2 포트 통계 18
_2.3 LOOP PROTECTION 19
_2.4 SERIAL 서버 상태 20
_2.5 SECURITY 21
_2.6P OE STATE 23
_2.7 LLDP STATE 24
_2.8 IGMP SNOOPING STATE 25
_2.9 DHCP SNOOPING STATE 26
_2.10 QINQ INFORMATION 27
_2.11LOOP DETECT STATE 28
_2.12ARP INFORMATION 29
3. CONFIGURATION 30
_3.1 VLAN 30
3.1.1 개요 30

3.1.1.1 VLAN 모드 31
3.1.12 포트 링크 유형 31
3.1.1.2 프레임 처리 방법 32
3.1.2 VLAN 설정 33
3.1.2.1 VLAN 생성 33
3.2 PORT 36
3.2.1 PORT CONFIGURATION 36
3.2.2 포트 확장 38
3.2.2.1 Rate Limiting 38
3.2.2.2 Storm Control 40
3.2.2.1 Isolation 42
3.2.3 PORT MIRRORING 43
3.2.4 PORT AGGREGATION 49
3.2.4.1 개요 49
3.2.5 PORT VIOLATION 52
3.3 스패닝 트리 53
3.3.1 개요 53
3.3.2 스패닝 트리 설정 54
3.4 ERPS 57
3.4.1 개요 57
3.5POE MANAGEMENT 65
3.5.1 개요 65
3.5.2 POE CONFIGURATION 65
3.6SECURITY 69
3.6.1 PORT SECURITY 69
3.6.1.1 개요 69
3.6.1.2 포트 보안 설정 70
3.6.2 IP SOURCE GUARD 73
3.6.3 DOT1X 78
3.6.4 MAC AUTH 85
3.6.5 RADIUS 88
3.7CONTROL 93

3.7.1 시리얼 서버 93
3.7.2 IO CONTROL 96
3.8LOOPDETCT 97
3.8.1 개요 97
4. ADVANCE 99
4.1LLDP 99
4.1.1 개요 99
4.1.2 LLDP 설정 100
4.2IGMP SNOOPING 105
4.2.1 IGMP SNOOPING 의 원리 105
4.2.2 IGMP SNOOPING 설정 106
4.3MAC MANAGEMENT 109
4.3.1 개요 109
4.3.2 MAC 주소 설정 110
4.4DHCP SNOOPING 113
4.4.1 개요 113
4.4.2 DHCP SNOOPING 설정 115
4.5QINQ 118
4.5.1 개요 118
4.5.2 QINQ 설정 119
4.6ACL 121
4.6.1 개요 121
4.6.2 ACL 설정 121
4.7QOS 128
4.7.1 개요 128
4.7.2 QOS 설정 128
4.8 DOS 134
4.8.1 개요 134
4.8.2 DOS 설정 135

4.9 ROUTE141
4.9.1 ARP 141
4.9.2 ROUTE 144
5. MAINTENANCE 148
5.1 SYSTEM 설정 148
5.1.1 HOST NAME 설정 148
5.1.2 서비스 활성화 149
5.1.3 MANAGEMENT IP 151
5.2 FILE MANAGEMENT 153
5.2.1 BASIC INFORMATION 153
5.2.2 IMAGE MANAGEMENT 154
5.2.3 CONFIGURATION MANAGEMENT 155
5.2.4 CONFIGURATION MANAGEMENT 156
5.2.5 PAGE PACKAGE MANAGEMENT 157
5.3 USER MANAGEMENT 158
5.4 TIME MANAGEMENT 159
5.4.1 시스템 시간 보기 159
5.4.2 시스템 시간 설정 160
5.4.3 NTP 서버 설정 161
5.5 SNMP 162
5.6 SYSLOG SERVER 164
5.6.1 개요 164
5.6.2 SYSLOG 설정 165
6. DIAGNOSIS 167
6.1 NETWORK UTILITIES 167
6.1.1 개요 167
6.1.2 DIAGNOSTIC TOOL OPERATION 169
6.2OPTICAL TRANSCEIVER INFORMATION 171
6.2.1 OPTICAL TRANSCEIVER INFORMATION 보기 171

6.2.2 DETAIL INFORMATION 172
6.3 ONE-CLICK COLLECTION 173
6.4 DYING GASP 174
6.4.1 개요 174
6.4.2 DYING GASP 설정 175
6.5 CABLE DETECT 176

1. Web Overview

1.1 개요

MV-Series 제품은 웹 기반 네트워크 관리 기능을 제공하며 장치의 운영 및 유지 관리를 용이하게 합니다. 관리자는 웹 기반 설정 인터페이스를 통해 네트워크 장비를 시각적으로 관리하고 유지할 수 있습니다.

제품은 기본적으로 웹 기반으로 설정을 통한 간편하고 빠른 설정 및 사용자 편의성을 제공합니다.

해당 메뉴얼은 MV-Series 제품의 기본적은 동작 및 설정 방법 등을 설명하고 있습니다.

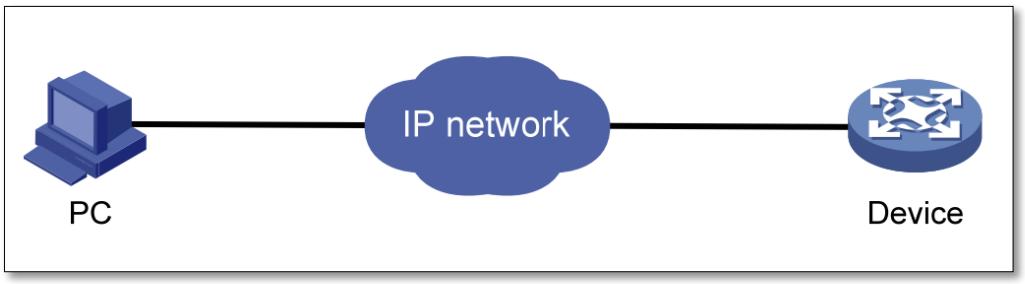


그림 1- 1 웹 기반 네트워크 관리 운영

1.2 웹 접속 방법

스위치는 기본 웹 로그인 정보가 제공됩니다. 다음의 기본 정보를 사용하여 웹 인터페이스에 로그인할 수 있습니다.

- 사용자 이름: admin
- 비밀번호: admin
- IP 주소: 192.168.168.1

웹 인터페이스를 통해 장치에 로그인 하려면:

1. 이더넷 케이블을 사용하여 장치의 이더넷 인터페이스를 PC 에 연결합니다.
2. PC 의 IP 주소를 설정하고 PC 와 장치가 서로 올바르게 통신할 수 있는지 확인합니다.
3. PC 의 IP 주소를 네트워크 세그먼트 192.168.168.0/24(192.168.168.1 제외) 내의 주소로 설정합니다(예: 192.168.56.2).
4. 브라우저를 열고 로그인 정보를 입력합니다.
5. PC 에서 브라우저를 열고 주소 표시줄에 IP 주소 http://192.168.168.1 을 입력한 후 Enter 를 누르면 그림과 같이 웹 인터페이스의 로그인 페이지로 들어갈 수 있습니다. 그림 1-2 처럼 사용자 이름 admin 과 비밀번호 admin 을 입력하고 로그인을 클릭합니다.

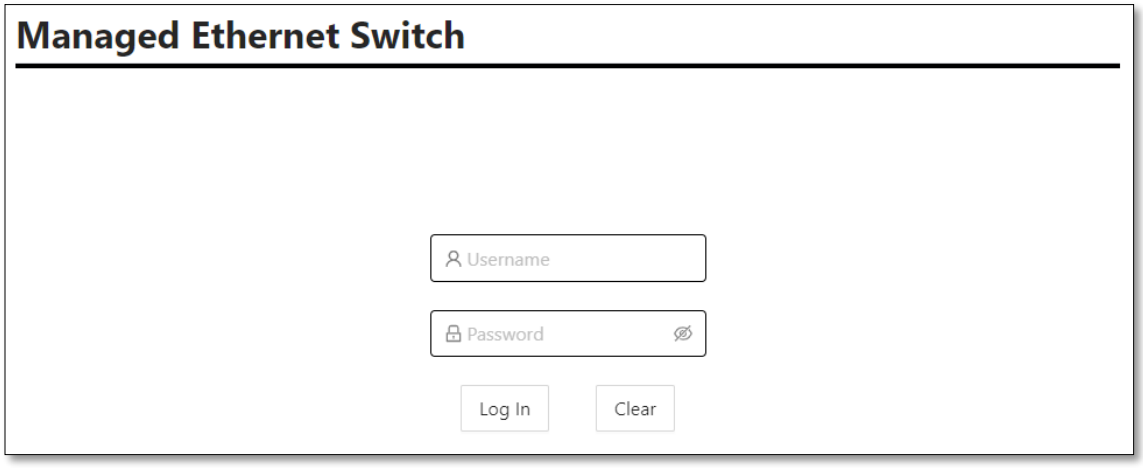


그림 1- 2

1.3 웹에서 로그아웃

그림과 같이 웹 기반 네트워크 관리를 종료하려면 로그아웃 버튼을 클릭하세요.

웹 인터페이스에서 로그아웃하기 전에는 시스템이 현재 설정을 저장하지 않습니다. 따라서 로그아웃하기 전에 현재 설정을 저장하는 것이 좋습니다.

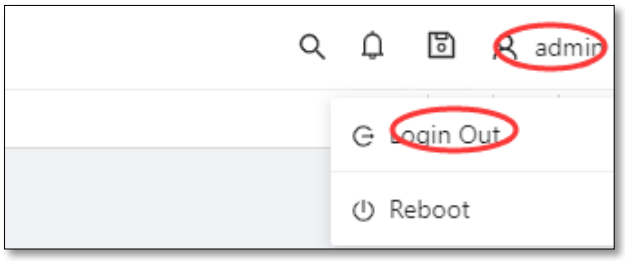


그림 1- 3 로그아웃

NOTE:

- 브라우저를 직접 닫아서 로그아웃 할 수 없습니다.

1.4 설정 저장

설정 저장은 스위치 재시작시 현재 설정을 설정 파일에 저장하는 기능을 제공합니다.

다음과 같은 아이콘을 클릭하여 현재 설정을 설정파일에 저장합니다.

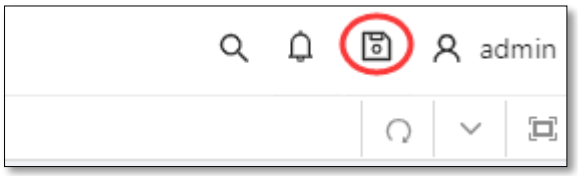


그림 1- 4 설정 저장

1.5 Reboot

Reboot 버튼을 클릭하면 장치가 재부팅 됩니다.

NOTE:

- 장치를 재부팅 하기 전에 설정을 저장하세요. 그렇지 않으면 장치가 다시 부팅된 후 저장되지 않은 모든 설정이 손실됩니다. 장치가 다시 부팅된 후에는 웹 인터페이스에서 다시 로그인 해야 합니다.

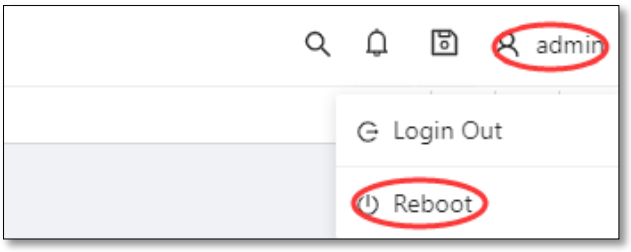


그림 1- 5 재부팅

1.6 웹 인터페이스

웹 인터페이스는 3 가지 영역으로 나뉘며 메뉴 탐색, 보조 영역, 본문 영역으로 구분합니다.

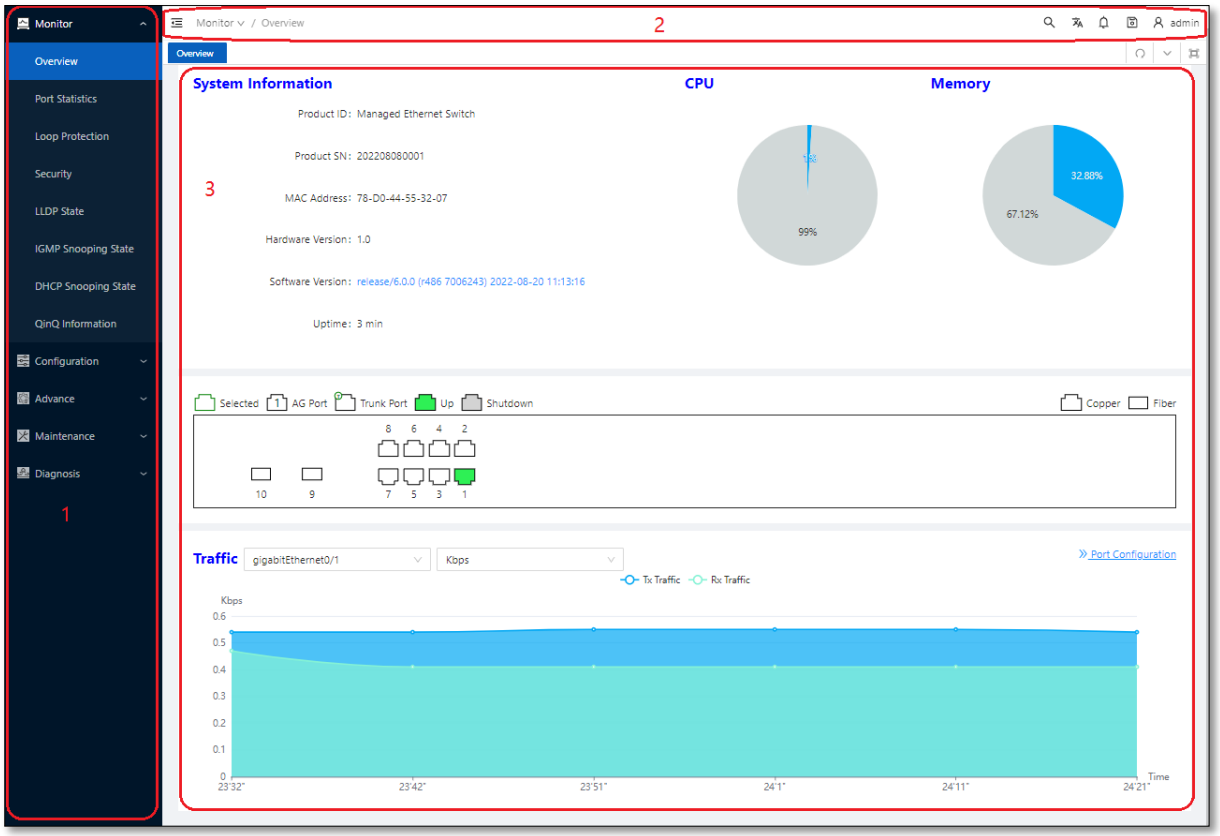


그림 1- 6 웹 기반 인터페이스

- 메뉴 탐색: 1 번 영역으로 필요에 따라 메뉴를 선택할 수 있습니다. 선택 후 결과는 본문 영역에서 확인할 수 있습니다.
- 보조 영역: 메뉴 검색, 알람 메시지, 프롬프트, 저장, 종료, 재부팅당 기타 작업을 할 수 있습니다.
- 본문 영역: 설정을 진행할 수 있으며 메뉴 선택에 따른 정보를 확인할 수 있습니다.

1.7 웹 기반 기능 소개

표 1-1 은 웹 기반 관리 기능을 설명합니다.

메뉴/탭			기능설명
Monitor	Overview		장치의 MAC 주소, 일련 번호, 소프트웨어 및 하드웨어 버전, CPU 사용량, 운영체제 등을 표시합니다.
	Port statistics		포트 수 표시
	Loop protection		장치의 루프 보호 상태를 표시합니다.
	Security		장치의 보안 클래스 관련 상태를 표시합니다.
	Serial server state		장치의 시리얼 포트 서버의 동작 상태를 표시합니다.
	LLDP Status		장치의 LLDP 동작 상태 표시
	IGMP Snooping State		장치의 IGMP 스누핑 상태 표시
	DHCP Snooping State		장치의 DHCP 스누핑 상태 표시
	QinQ information		디스플레이 장치 QinQ 상태
Configuration	VLAN		VLAN 생성, 수정, 삭제, 포트 속성 및 VLAN 속성 설정
	Port	port configuration	포트 관련 속성 설정
		port extension	포트 속도 제한, storm 억제, 포트 격리 설정
		port mirroring	포트 미러링 추가/제거
		Port aggregation	포트 추가/삭제
	Spanning tree		STP, RSTP, MSTP 기능 설정
	ERPS		ERPS 설정
	PoE		PoE 설정
	Security	port security	포트 보안 기능 설정 및 삭제
		IP Source Guard	IP Source Guard 기능 설정 및 삭제
		Dot1x	802.1X 인증 설정
		MAC authentication	MAC 인증 프로필 설정
		RADIUS	RADIUS 서버 설정
	Control	Serial Server	직렬 서버 설정
		IO control	DI, DO 설정
Advance	Layer 2	LLDP	장치의 LLDP 기능 설정 및 삭제

		configuration	
		IGMP Snooping Configuration	IGMP 스누핑 표시/설정
		MAC configuration	장치의 MAC 주소 관리 모드 설정
		DHCP Snooping Configuration	장치에서 DHCP 스누핑 설정
		QinQ configuration	장치의 QinQ 기능 설정
	Security	ACL configuration	장치의 ACL 기능 설정
		QoS configuration	장치의 QoS 기능 설정
Diagnosis	System Configuration		장치의 telnet, ssh, http, https 기능을 활성화/비활성화 합니다.
	File Management		펌웨어 업그레이드 관리, 설정관리, 인증서 관리, 페이지 패키지 관리
	User Management		사용자 생성/삭제, 사용자 비밀번호 설정
	Time Management		시스템 현재 날짜 및 시간 표시/설정
	SNMP		SNMP 설정 생성, 수정, 삭제
	Network Utility		ping/trace 경로 작업을 실행하고 실행 결과를 표시합니다.
	Transceiver Information		제조업체 정보, 일련번호, 광 파워 등 광모듈 정보 확인
	One-click collection		진단정보파일을 생성하고 로컬 호스트에서 보거나 저장하기 위해 파일을 다운로드 할 수 있습니다.

표 1- 1 기능 설명

2. Monitor

2.1 개요

Monitor 의 Overview 에 표시된 바와 같이 " System Information ", "Panel Port", "Traffic"의 3 개 섹션으로 구분됩니다.

1. " System Information " 페이지에서 장치의 제품 ID, 일련번호, MAC 주소, 하드웨어 및 소프트웨어 버전을 확인할 수 있습니다.

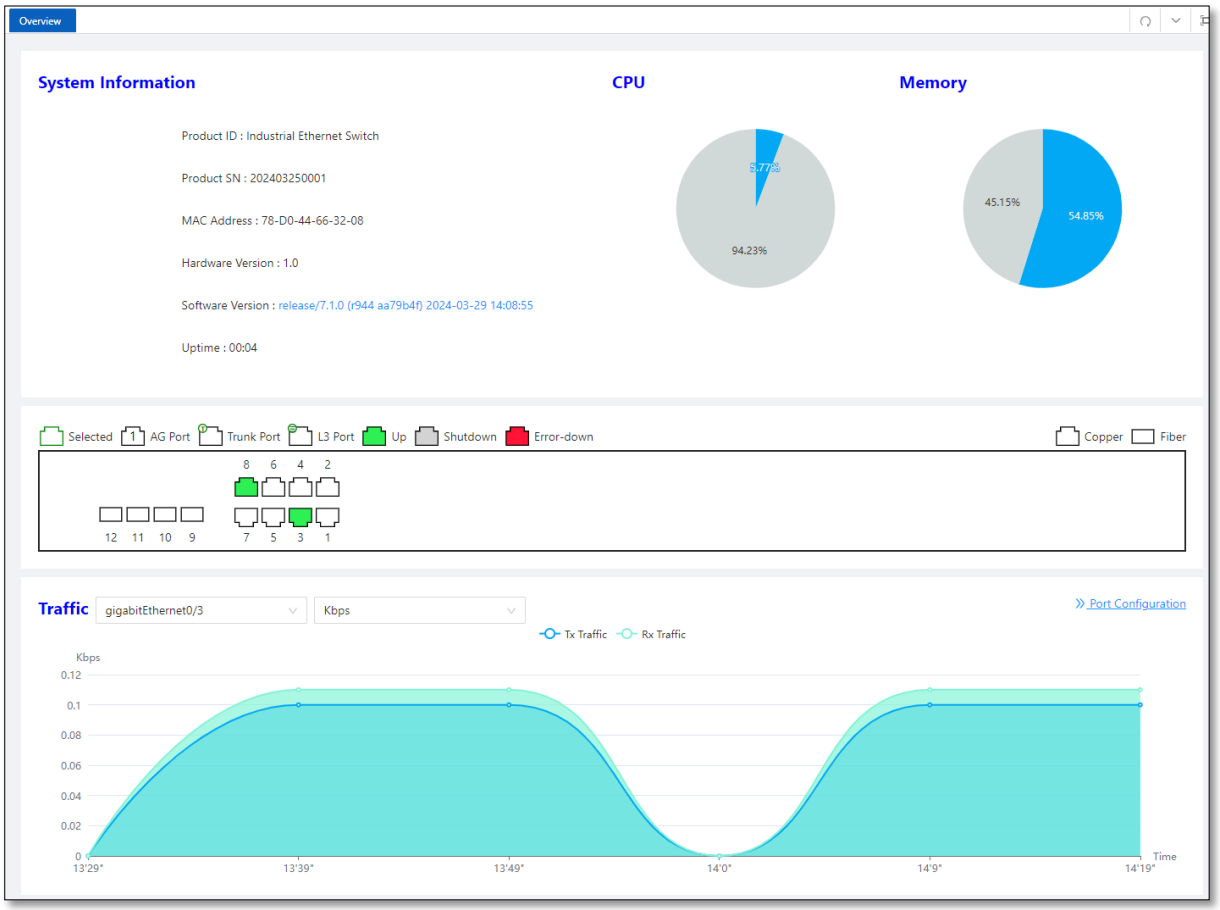


그림 2- 1 Overview 페이지

메뉴	설명
호스트 이름	장치 이름을 표시합니다. 사용자가 이를 변경할 수 있습니다.
MAC 주소	장치의 MAC 주소를 표시합니다.
하드웨어 버전	장치의 하드웨어 버전을 표시합니다.
소프트웨어 버전	장치의 소프트웨어 버전을 표시합니다.
출시일	장치 소프트웨어의 출시 날짜를 표시합니다.
제품번호	장치의 일련번호를 표시합니다.
CPU 사용량	CPU 사용량을 표시합니다.
이용가능한 메모리	장치의 메모리 상태를 표시합니다.
시스템 가동 시간	마지막 시스템 시작 이후의 시간을 표시합니다.

표 2- 1 기본 정보

1. " Panel Port " 페이지에서는 장치의 패널 다이어그램과 패널 포트의 동작 조건을 볼 수 있습니다.
2. " Traffic " 페이지에서는 포트의 트래픽을 관찰할 수 있습니다.

2.2 포트 통계

포트 통계는 수신 및 전송된 패킷에 대한 통계를 표시합니다.

Monitor> Port Statistics 탐색 영역에서 다음에 표시된 페이지로 들어갑니다. 그림 2-2 페이지에는 포트의 RX 로드가 표시되며 TX 로드, 속도 CRC, 오류 충돌중인 횟수 등이 표시됩니다.

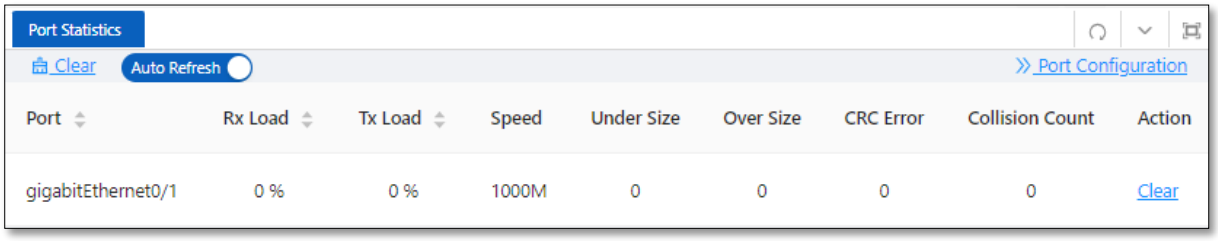


그림 2- 2 포트 통계 페이지

메뉴	설명
Port	논리적 인터페이스의 이름입니다.
Rx Load	포트의 Rx 로드입니다..
Tx Load	포트의 Tx 로드입니다.
Speed	포트 가동률
Under Size	포트에서 수신한 패킷 수가 64 바이트 미만입니다.
Over Size	포트에서 수신한 패킷 수가 최대 MTU 설정보다 큽니다.
CRC Error	CRC 검사 오류로 인해 수신된 패킷 수
Collision Count	포트에서 수신한 충돌 패킷 수
Clear	포트 통계 삭제

표 2- 2 포트 통계 메뉴

2.3 Loop Protection

" Loop Protection " 페이지는 ERPS 및 스패닝 트리 프로토콜과 같은 루프 관련 프로토콜의 동작 상태를 표시하는 데 사용됩니다.

1. Monitor > Loop Protection 메뉴에서 Loop Protection 상태 페이지를 확인합니다.
2. 활성화된 ERPS 및 스패닝 트리 프로토콜의 동작 상태를 확인할 수 있으며, 특정 설정 값은 프로토콜의 관련 섹션에서 설정할 수 있습니다.
3. ERPS 설정 그리고 스패닝 트리 설정 관련 설정 인터페이스로 전환할 수 있습니다.

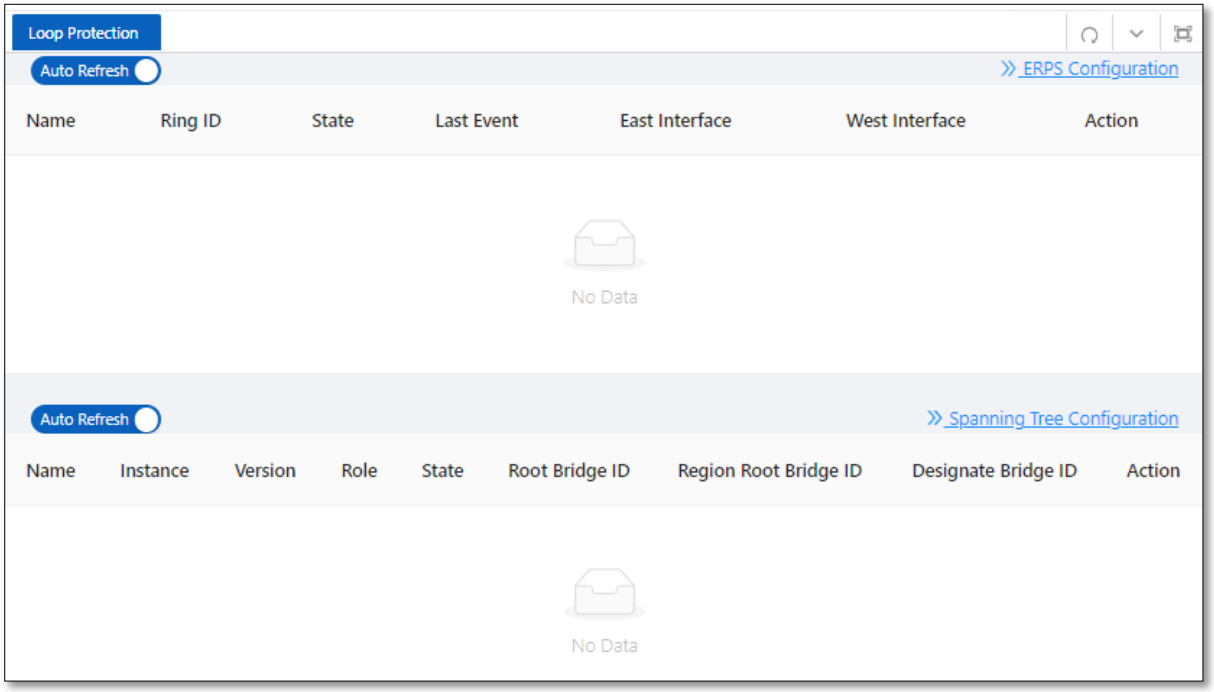


그림 2- 3 Loop Protection 상태

2.4 Serial 서버 상태

" Serial Server State " 페이지는 시리얼 서버의 동작 상태를 표시하는 데 사용됩니다.

1. Monitor > Serial Server State 메뉴에서 다음과 같이 시리얼 서버 상태 페이지로 접속합니다.



그림 2- 4 시리얼 서버 상태

2. 시리얼 동작 상태를 확인할 수 있습니다.

메뉴	설명
ID	직렬 포트 서버의 직렬 포트 ID 번호
Net Octets Rx	네트워크가 수신한 바이트 수
Net Packets Rx	네트워크에서 수신한 패킷 수
Net Octets Tx	네트워크에서 보낸 바이트 수
Net Packets Tx	네트워크에서 보낸 패킷 수
Serial Octets Rx	직렬 포트에서 수신한 바이트 수
Serial Packets Rx	직렬 포트에서 수신한 패킷 수
Serial Octets Tx	직렬 포트에서 보낸 바이트 수
Serial Packets Tx	직렬 포트에서 보낸 패킷 수
Net Connect Up/Down times	네트워크 연결 수
Serial Overload Drop Packets	직렬 포트 오버플로로 인해 폐기된 패킷 수

표 2- 3 시리얼 서버 메뉴

3. 시리얼 설정을 진행하려면 Configuration 을 클릭합니다.

2.5 Security

" Security " 페이지는 포트 보안, IP 소스 가드, MAC 인증의 세 부분으로 장치 보안 관련 프로토콜의 동작 상태를 표시하는 데 사용됩니다.

1. Monitor > Security 메뉴에서 화면과 같이 보안 표시 페이지로 접속합니다.

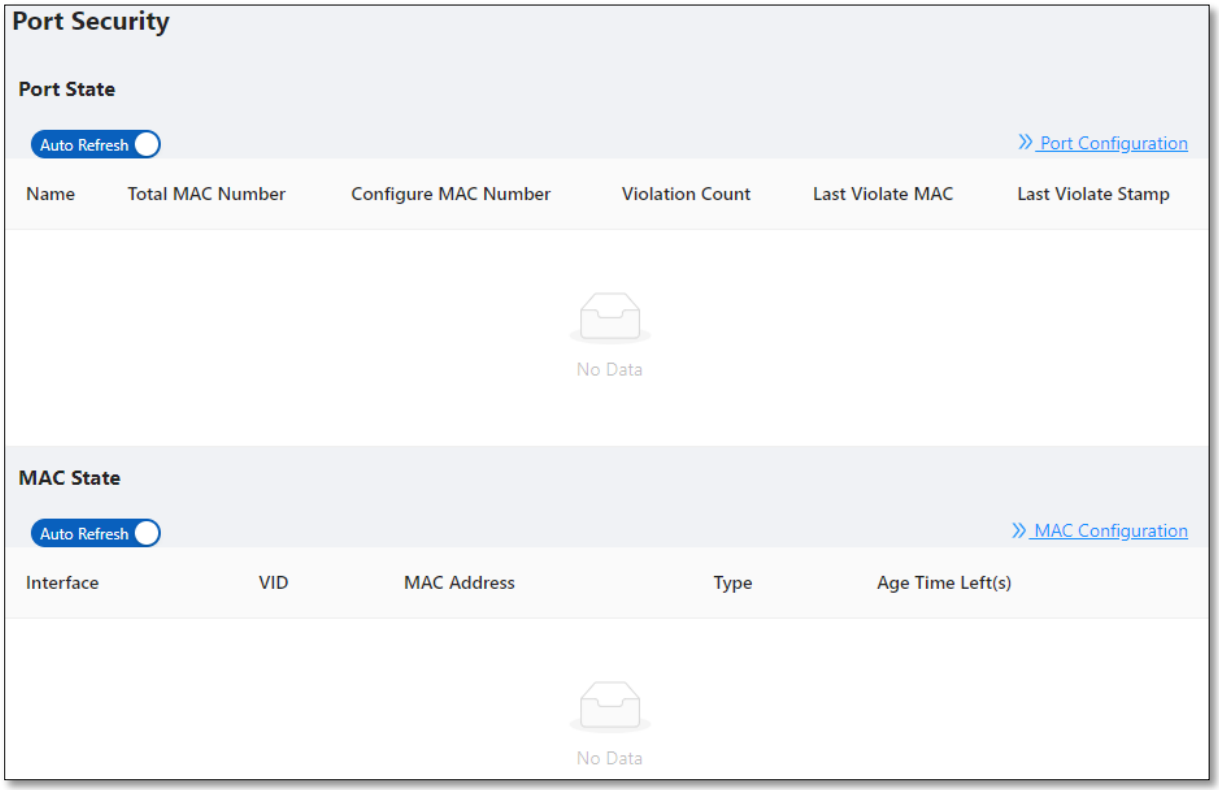


그림 2- 5 Port Security 상태

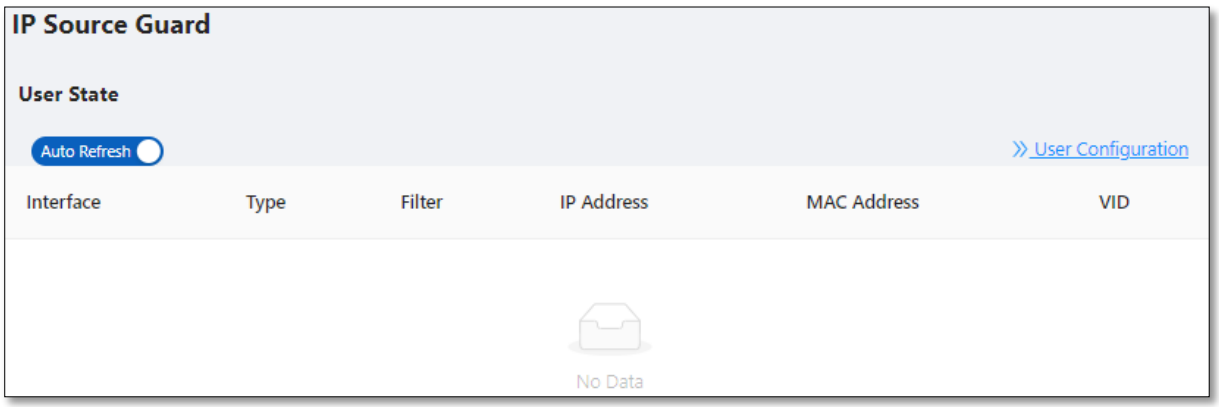


그림 2- 6 IP Source Guard 상태

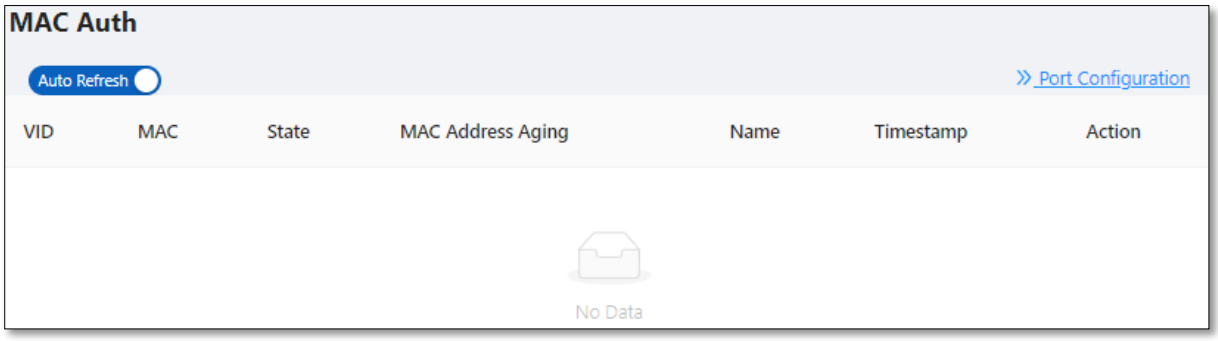


그림 2- 7 MAC Auth 상태

2. 해당 설정화면에서 ERPS, 스패닝 트리, IP 소스 가드, MAC 인증의 작동 상태를 볼 수 있으며, 구체적인 매개변수는 프로토콜의 관련 섹션에서 설명할 수 있습니다.

3. 각 Configuration 을 클릭하면 해당 설정 페이지로 전환됩니다.

2.6 PoE State

" PoE State" 메뉴에서 PoE 상태를 확인할 수 있습니다.

1. Monitor > PoE State 메뉴에서 PoE 상태를 확인합니다.

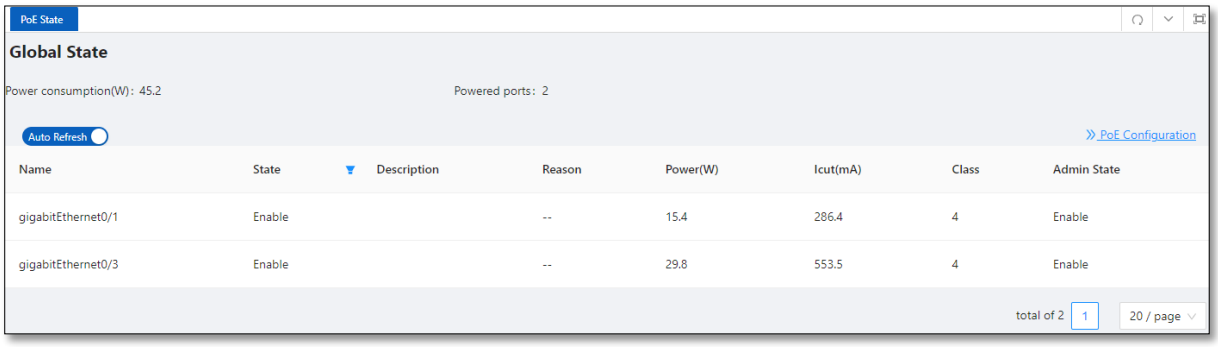


그림 2- 8 PoE State

2. 현재의 페이지에서는 장치의 전체 전원 공급량, 전원 공급 포트 수, 등 상태를 확인합니다.

메뉴	설명	
Global State	Power Consumption(w)	현재 PoE 장치의 외부 전원 공급 장치
	Powered ports	전원 공급된 포트 수
Port	Name	포트 번호
	State	PoE 현재 전원 공급 상태, disable: 전원 꺼진 상태 enable: 전원 공급 상태
	Description	PoE 포트설명
	Reason	포트에서 전원을 공급할 수 없는 이유는 Short: 부하가 짧음 Management: 전력 부족
	Power(W)	포트에서 소비되는 전력
	Icut(mA)	현재 포트의 동작 전류
	Class	이 포트에 연결된 PD 장치의 클래스
	Admin State	이 포트의 PoE 기능이 활성화 또는 비활성화되었는지 표시

표 2- 4 PoE 상태 메뉴

2.7 LLDP State

"LLDP State"는 장치의 LLDP 상태를 확인할 수 있습니다.

1. Monitor > LLDP State 메뉴에서 다음과 같이 LLDP 상태 페이지로 접속합니다.
2. 페이지에서 활성화된 LLDP 프로토콜의 동작 상태를 확인할 수 있으며 LLDP 설정은 관련 설정 페이지에서 진행할 수 있습니다.
3. LLDP Configuration 을 클릭하면 설정화면으로 전환됩니다.

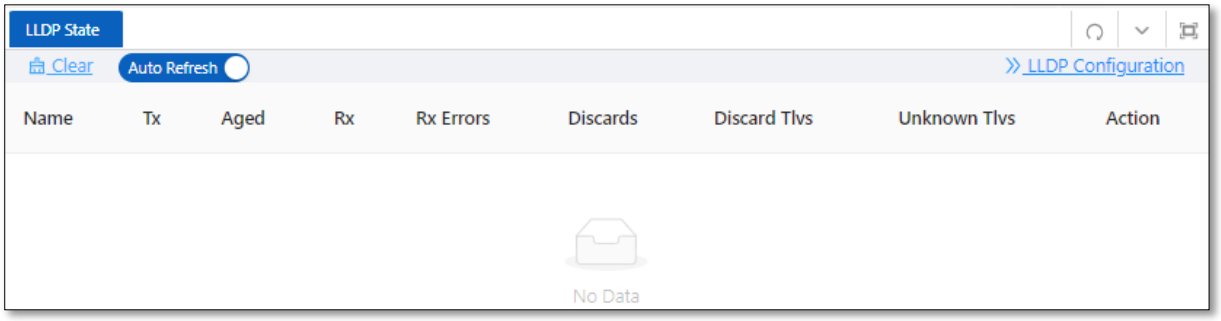


그림 2- 9 LLDP 상태

2.8 IGMP Snooping State

" IGMP Snooping State " 페이지는 장치의 IGMP Snooping 프로토콜의 동작 상태를 확인할 수 있습니다.

1. "Monitor > IGMP snooping State" 메뉴에서 IGMP Snooping State 로 접속합니다.
2. IGMP Snooping 프로토콜의 동작 상태를 확인할 수 있습니다.
3. IGMP Snooping Configuration 을 클릭하면 설정 화면으로 전환됩니다.

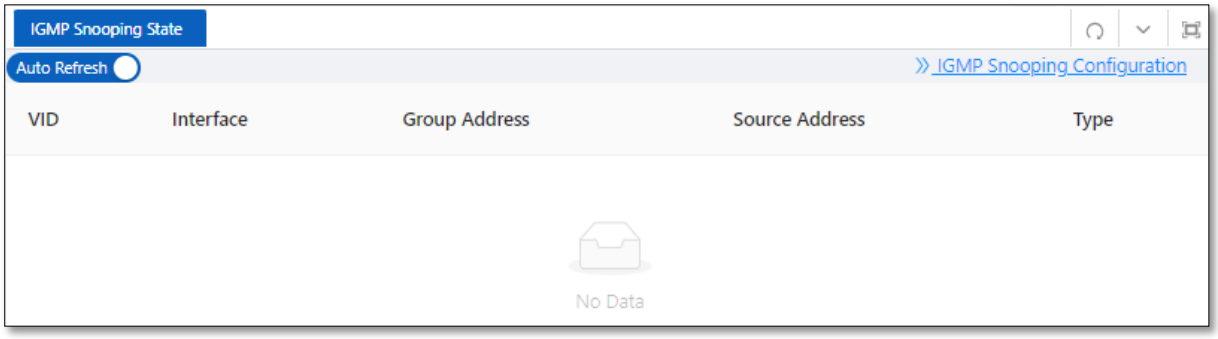


그림 2- 10 IGMP Snooping 상태

2.9 DHCP Snooping State

" DHCP Snooping State " 페이지는 장치의 DHCP Snooping 프로토콜의 동작 상태를 확인할 수 있습니다.

1. Monitor > DHCP Snooping State 메뉴에서 다음과 같이 DHCP Snooping 상태 페이지로 접속합니다.

2. 페이지에서 활성화된 DHCP Snooping 프로토콜의 동작 상태를 확인할 수 있습니다.

3. DHCP Snooping Configuration 버튼을 클릭하면 설정화면으로 전환됩니다.

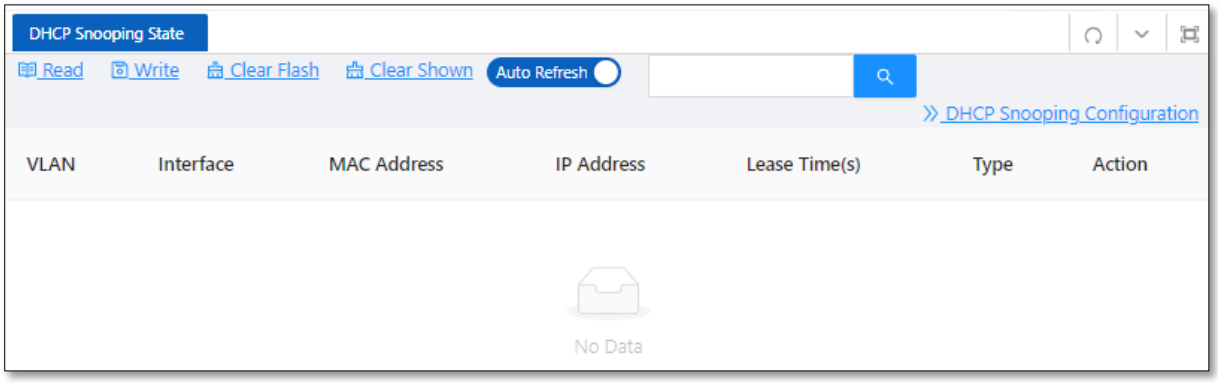


그림 2- 11 DHCP Snooping State

2.10 QinQ Information

" QinQ Information " 페이지는 장치 QinQ 정보의 동작 상태를 확인할 수 있습니다.

1. Monitor > QinQ Information 메뉴에서 QinQ 상태 페이지로 접속합니다.
2. 페이지에서 켜져 있는 QinQ 의 동작 상태를 확인할 수 있습니다.
3. QinQ Configuration 버튼을 클릭하면 QinQ 설정 화면으로 전환됩니다.

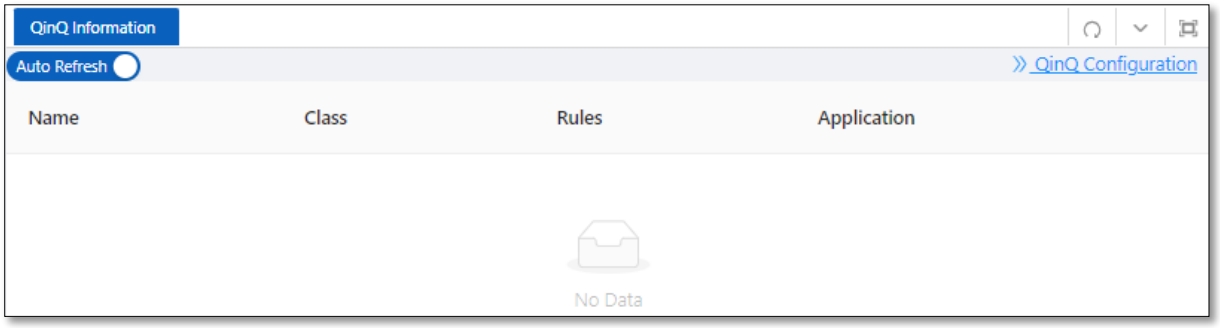


그림 2- 12 QinQ information

2.11 Loop Detect State

"Loop Detect State" 페이지는 장치의 Loop Detect State 동작 상태를 확인할 수 있습니다.

1. Monitor > Loop Detect State 메뉴에서 Loop Detect State 페이지로 접속합니다.
2. 작업상태를 확인할 수 있습니다. 루프 감지 기능이 켜져 있는지 확인할 수 있습니다.
3. Loop Detect Configuration 버튼을 클릭하면 설정화면으로 전환합니다.

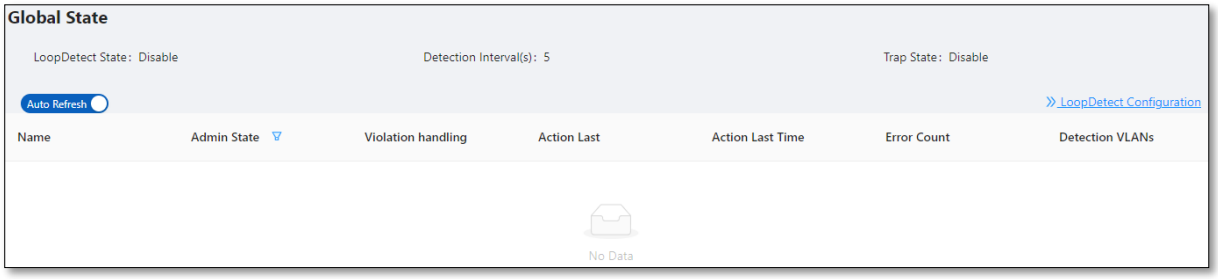


그림 2- 13 Loop Detect State

2.12 ARP Information

" ARP Information " 페이지는 장치의 ARP 정보 동작 상태를 확인할 수 있습니다.

1. Monitor > ARP/Neighbor Information 을 선택하여 그림 2-14 와 같이 ARP/Neighbor 상태 페이지로 들어갑니다.
2. 페이지에서 켜진 ARP/Neighbor 의 작동 상태를 볼 수 있으며, 프로토콜의 관련 섹션에서 구체적인 설정값을 확인할 수 있습니다.
3. ARP/Neighbor Configuration 버튼을 클릭하여 ARP/Neighbor Configuration 페이지로 전환합니다.

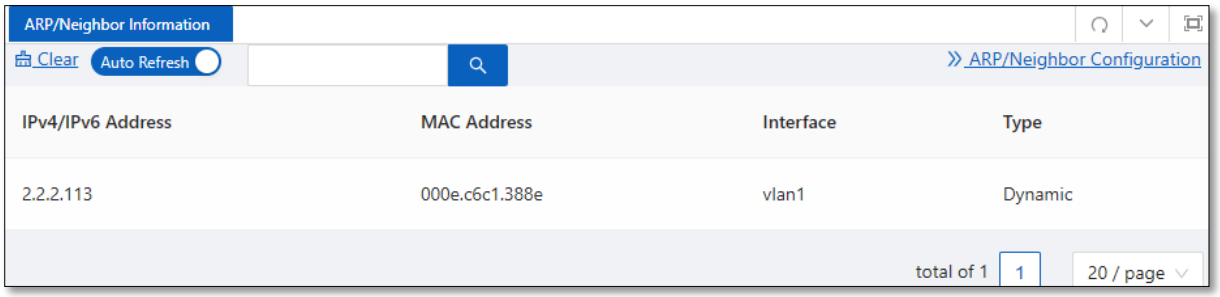


그림 2- 14 ARP Information

3. Configuration

3.1 VLAN

3.1.1 개요

이더넷은 CSMA/CD(Carrier Sense Multiple Access/Collision Detect) 메커니즘을 기반으로 하는 네트워크 기술입니다. 매체가 공유되므로 이더넷에서는 충돌과 과도한 브로드캐스트가 흔히 발생합니다. 이 문제를 해결하기 위해 가상 LAN(VLAN)이 도입되었습니다. 동일한 VLAN 에 할당된 포트 간에 프레임이 전환되는 레이어 2 브로드캐스트 도메인으로 나누는 것입니다. VLAN 은 레이어 2 에서 서로 격리됩니다. VLAN 은 브리징 도메인이며 모든 브로드캐스트 트래픽은 그림과 같이 그 안에 포함됩니다.

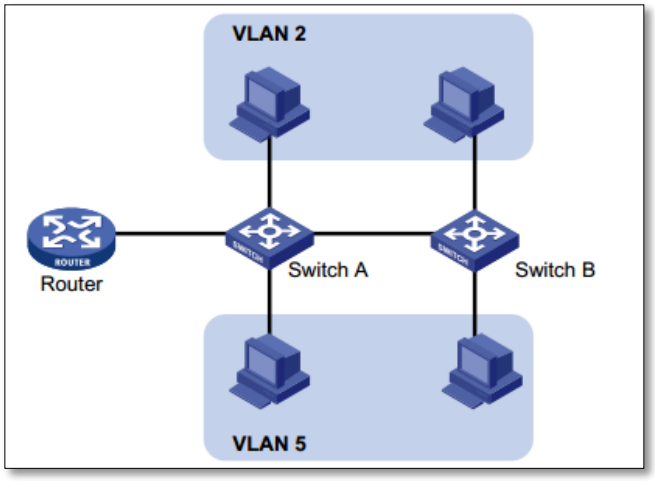


그림 3- 1 VLAN 블록도

VLAN 은 물리적 기반이 아닌 조직 기반으로 논리적으로 구분됩니다. 예를 들어, 특정 작업 그룹에서 사용하는 모든 워크스테이션과 서버는 물리적 위치에 관계없이 동일한 LAN 에 연결될 수 있습니다. VLAN 기술은 다음과 같은 이점을 제공합니다.

- 개별 VLAN 내에서 브로드캐스트 트래픽을 제한합니다. 이는 대역폭 낭비를 줄이고 네트워크 성능을 향상시킵니다.
- LAN 보안 향상. 사용자 그룹을 다른 VLAN 에 할당하면 이를 layer 2 에서 격리할 수 있습니다. 서로 다른 VLAN 에 있는 호스트가 통신하려면 라우터 또는 layer 3 스위치가 필요합니다.

- 유연한 가상 작업 그룹 생성. 동일한 워크그룹의 사용자는 물리적 위치에 관계없이 동일한 VLAN 에 할당될 수 있으므로 네트워크 구축 및 유지 관리가 훨씬 쉽고 유연해집니다.

다음을 기반으로 VLAN 을 생성할 수 있습니다.

- 포트
- MAC 주소
- 프로토콜
- IP 서브넷
- 정책
- 기타 기준

포트기반 VLAN 을 사용할 수 있으며 이 장에서는 포트 기반 VLAN 에 대해서만 설명합니다.

3.1.1.1 VLAN 모드

태그 처리 모드에 따라 포트의 VLAN 모드는 다음 세 가지 중 하나일 수 있습니다.

- Access : 액세스 포트는 하나의 VLAN 에만 속하며 일반적으로 사용자 장치에 연결됩니다.
- Trunk : 트렁크 포트는 여러 VLAN 에 가입하여 트래픽을 수신하고 보낼 수 있습니다. 일반적으로 네트워크 장치에 연결됩니다.
- Hybrid : 하이브리드 포트는 여러 VLAN 에 가입하여 트래픽을 수신하고 보낼 수 있습니다. 사용자 장치 또는 네트워크 자치를 연결할 수 있습니다.

하이브리드 포트는 다음과 같은 점에서 트렁크 포트와 다릅니다.

- 하이브리드 포트를 사용하면 여러 VLAN 의 트래픽이 태그 없이 통과될 수 있습니다.
- 트렁크 포트는 기본 VLAN 의 트래픽만 태그 없이 통과하도록 허용합니다.

3.1.12 포트 링크 유형

기본적으로 VLAN 1 은 모든 포트의 기본 VLAN 입니다. 그러나 필요에 따라 포트의 기본 VLAN 을 변경할 수 있습니다.

- 액세스 포트는 하나의 VLAN 에만 가입할 수 있으므로 기본 VLAN 은 해당 포트가 속한 VLAN 이며 설정할 수 없습니다.

- 트렁크 또는 하이브리드 포트는 여러 VLAN 에 가입할 수 있으므로 해당 포트에 대한 기본 VLAN 을 설정할 수 있습니다.

3.1.1.2 프레임 처리 방법

포트 유형	작업(인 바운드 방향)		작업(아웃 바운드 방향)
	태그가 지정되지 않은 프레임	태그 된 프레임	
Access	기본 VLAN 태그를 사용하여 프레임을 지정합니다.	• VLAN ID 가 기본 VLAN ID 와 동일한 경우 프레임을 수신합니다. • VLAN ID 가 기본 VLAN ID 와 다른 경우 프레임을 삭제합니다.	기본 VLAN 태그를 제거하고 프레임을 보냅니다.
Trunk	포트에 기본 VLAN 이 있는지 확인하세요. • 그렇다면 기본 VLAN 태그를 사용하여 프레임에 태그를 지정합니다. 그렇지 않은 경우 프레임을 삭제하세요.	• 해당 VLAN 이 포트에 전달되는 경우 프레임을 수신합니다. 해당 VLAN 이 포트에 전달되지 않으면 프레임을 삭제합니다.	• 프레임이 기본 VLAN 태그를 전달하는 경우 태그를 제거하고 프레임을 보냅니다. • VLAN 이 포트에 전달되지만 기본 VLAN 과 다른 경우 태그를 제거하지 않고 프레임을 보냅니다.
Hybrid			해당 VLAN 이 포트에 전달되는 경우 프레임을 보냅니다. 프레임은 설정에 따라 VLAN 태그가 제거되거나 그대로 전송됩니다.

표 3- 1 VLAN 으로 설정된 포트 처리

3.1.2 VLAN 설정

3.1.2.1 VLAN 생성

1. Configuration > VLAN 메뉴에서 VLAN 설정 페이지로 접속합니다.

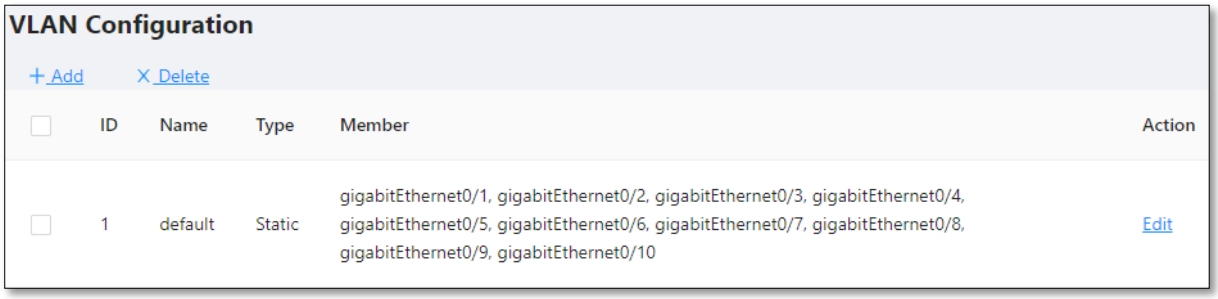


그림 3- 2 VLAN 설정

메뉴	설명
ID	이 필드에는 VLAN 의 ID 가 표시됩니다.
Name	기본적으로 VLAN 의 설명 문자열은 VLAN 0002 와 같은 VLAN ID 입니다.
Type	VLAN 유형을 표시 합니다.
Tagged Members	포트가 VLAN 태그를 제거하지 않고 VLAN 의 트래픽을 전송함을 나타냅니다.
Untagged Members	VLAN 태그를 제거하여 포트가 VLAN 의 트래픽을 전송함을 나타냅니다.
Edit	VLAN 편집 페이지로 들어가려면 클릭하세요.
Add	VLAN 추가 페이지로 들어가려면 클릭하세요.
Delete	VLAN ID 를 선택하고 클릭하여 삭제하세요.

표 3- 2 VLAN 설정 메뉴

2. Add 를 클릭하면 다음과 같이 VLAN 생성을 위한 페이지로 전환합니다.
3. ID 상자에 VLAN 번호를 입력합니다.
4. VLAN 이름을 입력합니다.
5. OK 를 클릭하여 구성을 완료하고 보조 영역에서 Save 를 클릭하여 해당 구성을 저장합니다.
6. VLAN 포트 멤버를 구성해야 하는 경우 Edit 버튼을 클릭하고 포트 패널에서 VLAN 에 가입하는 데 필요한 포트 멤버를 선택한 다음 OK 버튼을 클릭하여 작업을 완료합니다.



그림 3- 3 VLAN 생성

3.1.2.2 포트 설정

1. Configuration > VLAN 메뉴에서 VLAN 설정 페이지로 접속합니다.

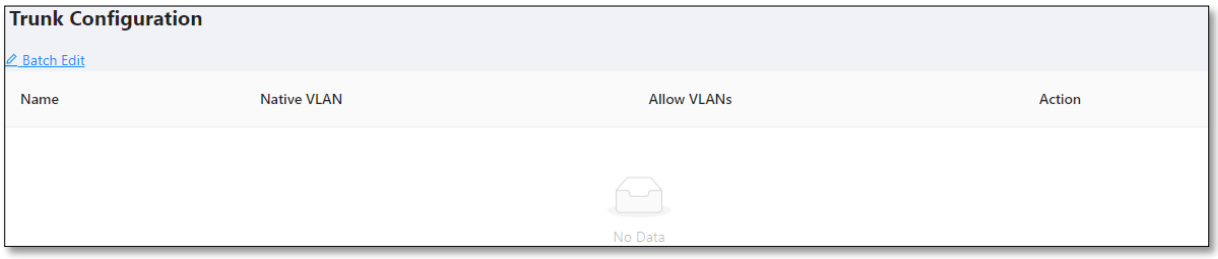


그림 3- 4 포트 설정

" Trunk Configuration " 아래의 Batch Edit 버튼을 클릭하여 그림과 같이 트렁크 설정 페이지로 접속합니다.

메뉴		설명
Mode	Access	포트의 VLAN 모드를 액세스로 설정합니다.
	Trunk	포트의 VLAN 모드를 트렁크로 설정합니다.
	Hybrid	포트의 VLAN 모드를 하이브리드로 설정합니다.
PVID		포트의 기본 VLAN ID 를 설정합니다. 액세스 모드에서만 존재합니다. • 링크의 두 끝에 있는 트렁크 포트는 동일한 PVID 를 가져야 합니다. 그렇지 않으면 링크가 패킷을 제대로 전송할 수 없습니다.
Native Vlan		VLAN(네이티브 Vlan), 트렁크 모드에만 존재합니다.
Allow VLANs		포트를 통해 허용되는 VLAN 을 선택합니다.

표 3- 3 트렁크 설정 설명

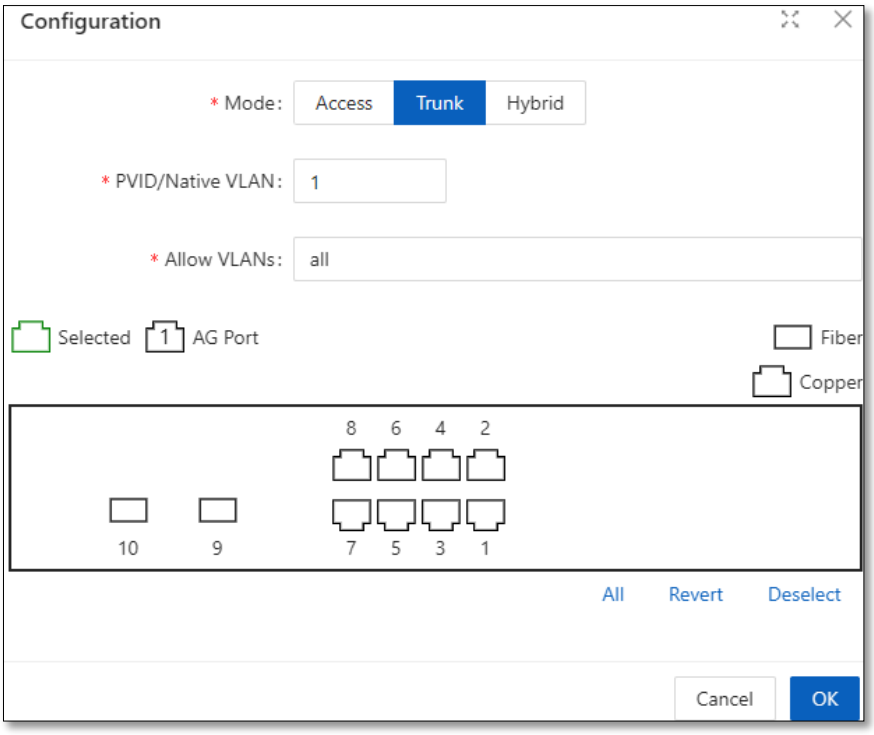


그림 3- 5 인터페이스 설정

2. VLAN 모드를 선택하고 PVID 및 VLAN 허용 상자에 VLAN 번호를 입력한 후 확인 버튼을 클릭하여 설정합니다.

3. 설정을 저장하려면 저장을 클릭합니다.

3.2 Port

3.2.1 Port Configuration

인터페이스 관리 기능을 사용하면 다음과 같이 인터페이스 정보 보기, 논리 인터페이스 생성/제거, 인터페이스 상태 변경, 인터페이스의 재설정 등을 수행할 수 있습니다.

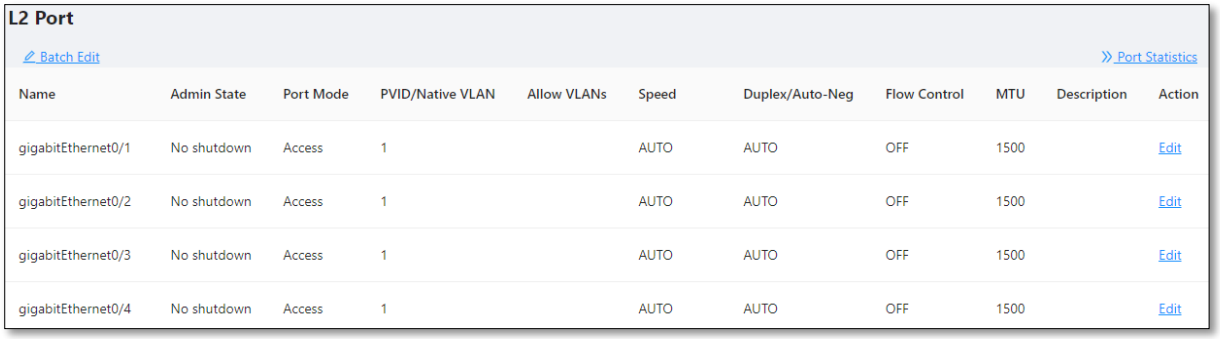


그림 3- 6 포트 설정 페이지

1. Configuration > Port > Port Configuration 메뉴에서 포트 설정 페이지로 접속합니다.
2. 설정할 포트를 선택하고 편집 버튼을 클릭하면 그림과 같이 인터페이스 설정 페이지로 전환합니다.

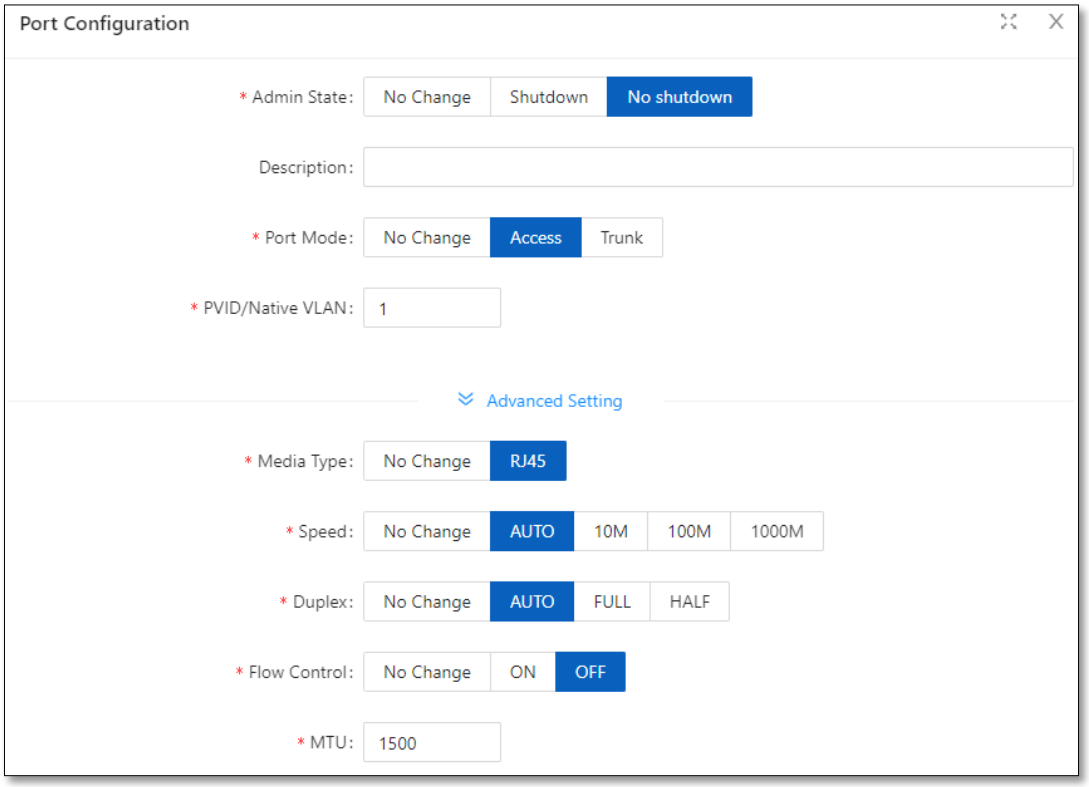


그림 3- 7 포트 설정

메뉴	설명
Admin State	포트를 종료/종료하지 않습니다.
Description	논리적인 인터페이스를 설정합니다.
Port Mode	포트의 VLAN 모드의 액세스 또는 트렁크 설정합니다.
PVID/Native VLAN	포트의 PVID 또는 기본 VLAN 을 설정합니다.
Medium type	콤보 포트의 중간 유형을 설정합니다. • RJ45: 포트 모드는 10/100/1000BASE-T 입니다. • SFP: 포트 모드는 1000BASE-X 입니다. 참고: 콤보 포트에만 해당됩니다.
Speed(copper)	포트의 전송 속도를 설정합니다. • 10: 10Mbps 를 나타냅니다. • 100M: 100Mbps 를 나타냅니다. • 1000M: 1000Mbps 를 나타냅니다. • 자동: 자동 협상을 나타냅니다. 참고: 이더넷 포트에만 해당됩니다.
Duplex(copper)	포트의 이중 모드를 설정합니다: • AUTO: 자동 협상을 나타냅니다. • FULL: 전이중을 나타냅니다. • HALF: 반이중을 나타냅니다. 참고: 이더넷 포트에만 해당됩니다.
Speed(fiber)	포트 모드 설정 • 100BASE-FX: 포트 모드가 100BASE-FX 임을 나타냅니다. • 1000BASE-X: 포트 모드가 1000BASE-X 임을 나타냅니다. • 2500BASE-X: 포트 모드가 2.5G BASE-X 임을 나타냅니다. • 10G BASE-X: 포트 모드가 10G BASE-X 임을 나타냅니다. 참고: SFP 포트에만 해당됩니다.
Autoneg(fiber)	포트의 자동 승인을 활성화하거나 비활성화합니다. 자동 협상 기능을 동시에 활성화하거나 비활성화해야 합니다. 시간을 피어 끝으로 설정합니다. 그렇지 않으면 링크 오류가 발생합니다. 참고: SFP 포트에만 해당됩니다.
Flow control	포트의 흐름 제어를 활성화하거나 비활성화합니다.
MTU	점보 프레임이 포트를 통과하는 것을 허용하거나 금지합니다.
Admin Shutdown	포트를 종료 또는 종료하지 않습니다.

표 3- 4 포트 설정 메뉴

3.2.2 포트 확장

3.2.2.1 Rate Limiting

포트 기반 속도 제한을 사용하면 스위치의 포트에 연결된 장치에서 네트워크 트래픽을 보내거나 받는 속도를 제한할 수 있습니다. 802.1p QoS(서비스 품질)와 달리 포트 기반 속도 제한은 유형을 기준으로 정보의 우선 순위를 지정하지 않습니다. 속도 제한은 단순히 스위치가 포트의 트래픽 속도를 줄여 설정한 제한을 초과하지 않도록 하는 것을 의미합니다. 포트의 속도 제한을 너무 낮게 설정하면 비디오 스트림 품질 저하, 온라인 활동 중 응답 시간 지연 및 기타 문제가 발생할 수 있습니다.

속도 제한을 가장 잘 활용하는 방법은 스위치에 연결된 우선순위가 낮은 장치가 대역폭을 너무 많이 사용하여 연결된 다른 장치의 속도를 늦추는 것을 방지하는 것입니다. 속도 제한과 QoS 를 결합하면 네트워크 효율성을 극대화하고 장치 및 활동의 우선순위를 지정하는 데 도움이 될 수 있습니다.

1. Configuration > Port > Port Extension > Rate Limiting 선택하여 다음과 같이 포트 속도 제한 페이지로 접속합니다.
2. "Rate Limiting(속도 제한)" 아래의 Batch Edit(일괄 편집) 버튼을 클릭하여 그림과 같이 속도 제한 설정 페이지로 접속합니다.

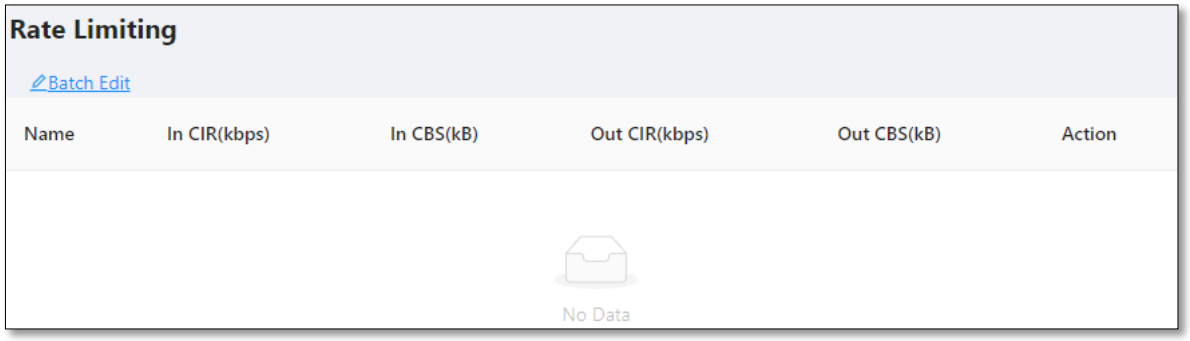


그림 3- 8 속도제한 페이지

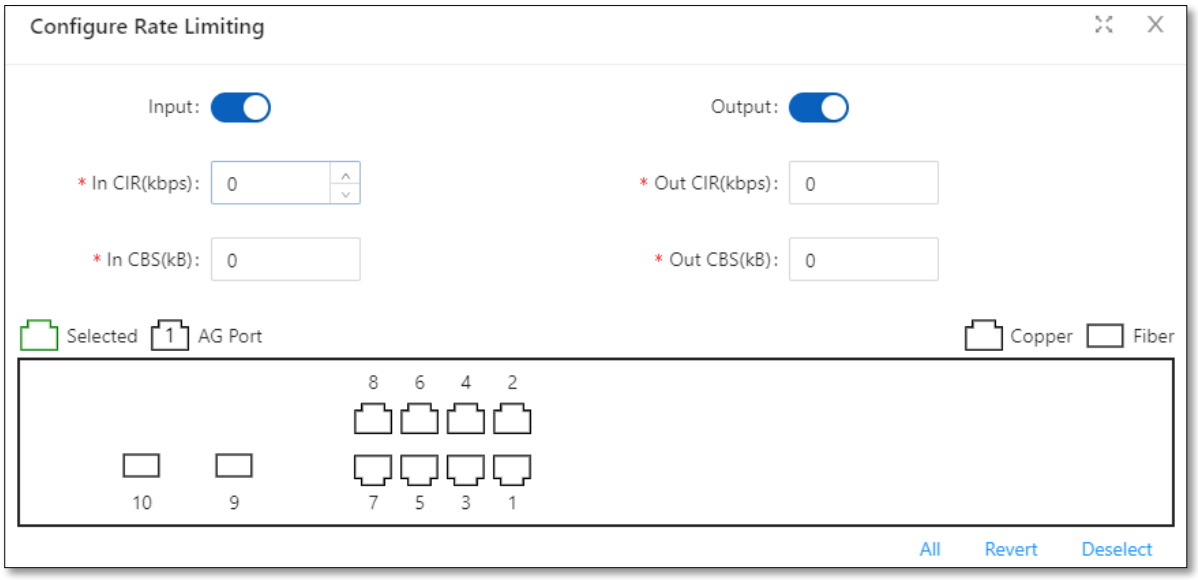


그림 3- 9 속도 제한 설정

NOTE:

- CBS 는 트래픽 정책을 위한 속도 제한 기능을 구합니다. CBS 로 트래픽을 폴리싱할 때 버스트 값은 제한 값의 4 배를 권장합니다. 버스트 값이 너무 낮으면 달성된 속도는 구성된 속도보다 훨씬 낮은 경우가 많습니다.

메뉴	설명
In CIR (kbps)	인 바운드 방향의 속도 제한을 지정합니다.(Kbits).
In CBS (KB)	인 바운드 방향의 버스트 크기 지정(Kbits).
Out CIR (kbps)	아웃 바운드 방향의 속도 제한을 지정합니다.(Kbits).
Out CBS (KB)	아웃 바운드 방향의 버스트 크기 지정(Kbits).

표 3- 5 포트 속도 제한 설정 메뉴

3.2.2.2 Storm Control

대량의 브로드캐스트, 멀티캐스트 또는 유니캐스트 패킷으로 인해 네트워크가 정체되면 트래픽 급증이 발생합니다. 스톰컨트롤 기능을 사용하면 이더넷 포트 보기 또는 포트 그룹 보기에서 인터페이스별로 특정 유형의 트래픽(현재 브로드캐스트, 멀티캐스트 및 알 수 없는 유니캐스트 트래픽)의 크기를 제한할 수 있습니다. 인터페이스 또는 포트 그룹 보기에서 인터페이스 또는 포트 그룹의 각 인터페이스를 통과할 수 있는 최대 브로드캐스트, 멀티캐스트 또는 알 수 없는 유니캐스트 트래픽을 설정합니다. 인터페이스의 브로드캐스트, 멀티캐스트 또는 알 수 없는 유니캐스트 트래픽이 임계값을 초과하면 시스템은 트래픽이 임계 값 아래로 떨어질 때까지 패킷을 삭제합니다.

1. Configuration > Port > Port Extension > Strom Control 을 선택하면 다음과 같이 설정 페이지로 접속합니다.

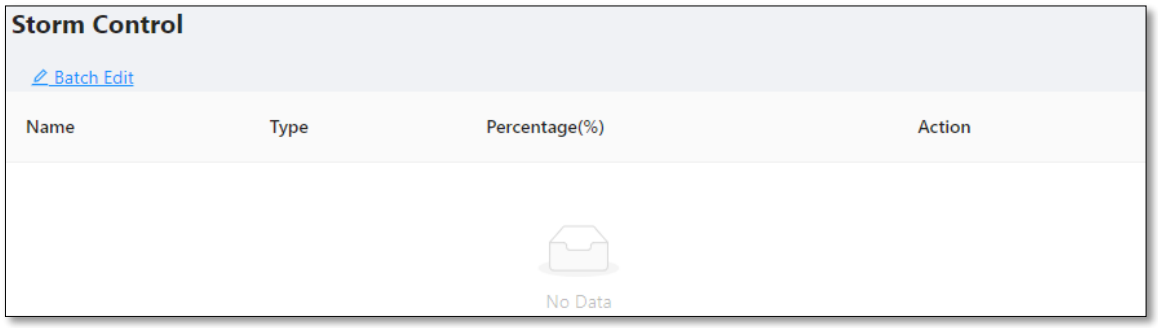


그림 3- 10 스톰제어 페이지

2. 유형을 선택하고 백분율 상자를 입력한 후 포트 패널에서 설정할 포트를 선택합니다.

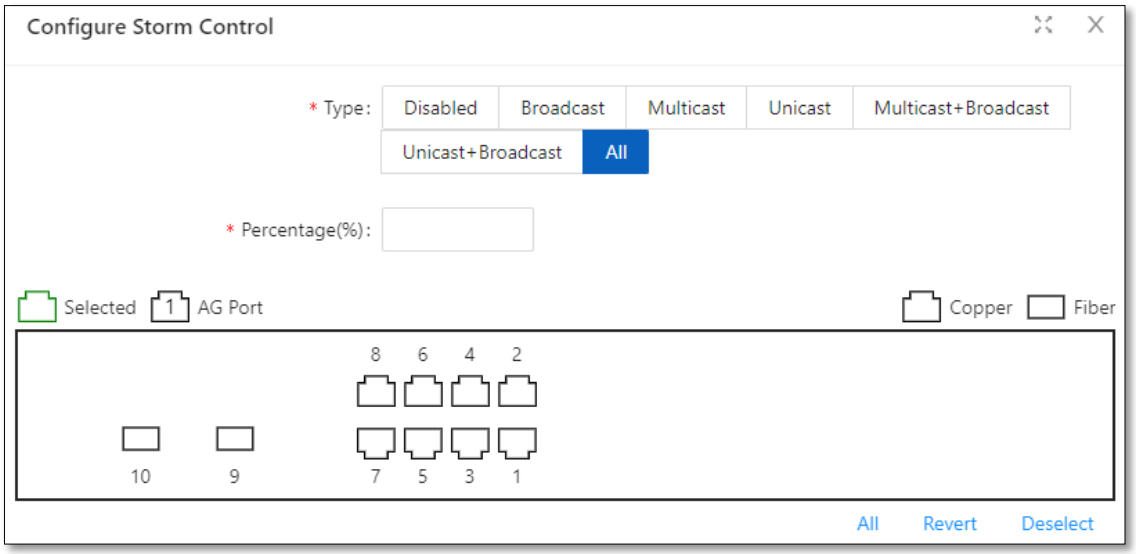


그림 3- 11 스톰제어 설정

메뉴		설명
Type	Disabled	스톰 컨트롤 기능을 비활성화 합니다.
	Broadcast	Broadcast 에 사용되는 설정 값을 선택하고 설정합니다. 백분율 상자의 값입니다.
	Multicast	멀티캐스트 제어에 사용되는 설정 값을 확인하고 설정합니다. 백분율 상자의 값입니다.
	Unicast	유니캐스트 제어에 사용되는 설정 값을 확인하고 설정합니다. 백분율 상자의 값입니다.
	multicast-broadcast	멀티캐스트 및 브로드 캐스트에 사용되는 설정 값을 선택합니다. 백분율 상자에 해당 값을 설정합니다.
	unicast-broadcast	유나 캐스트와 브로드 캐스트에 사용되는 설정 값을 선택합니다. 백분율 상자에 해당 값을 설정합니다.
	All	유나 캐스트와 멀티캐스트에 사용되는 설정 값을 선택하고, 브로드캐스트, 억제 및 백분율 상자에 해당 값을 설정합니다.
백분율(%)		전체 트래픽에 대한 최대 트래픽 비율을 나타냅니다. 이더넷 인터페이스의 전송 기능.

표 3- 6 스톰 제어 메뉴

3.2.2.1 Isolation

일반적으로 layer2 트래픽의 격리는 포트를 다른 VLAN 으로 할당하여 목적을 이룰 수 있습니다. VLAN 리소스를 절약하기 위해 위해 VLAN 내의 포트를 격리하는 포트 격리 기능이 도입되어 유연성과 보안이 향상됩니다.

1. Configuration > Port > Port Extension > Isolation 메뉴에서 Isolation 페이지로 접속합니다.
2. 격리할 포트를 선택하고 확인 버튼을 클릭합니다.
3. 설정 완료 후 저장을 클릭합니다.

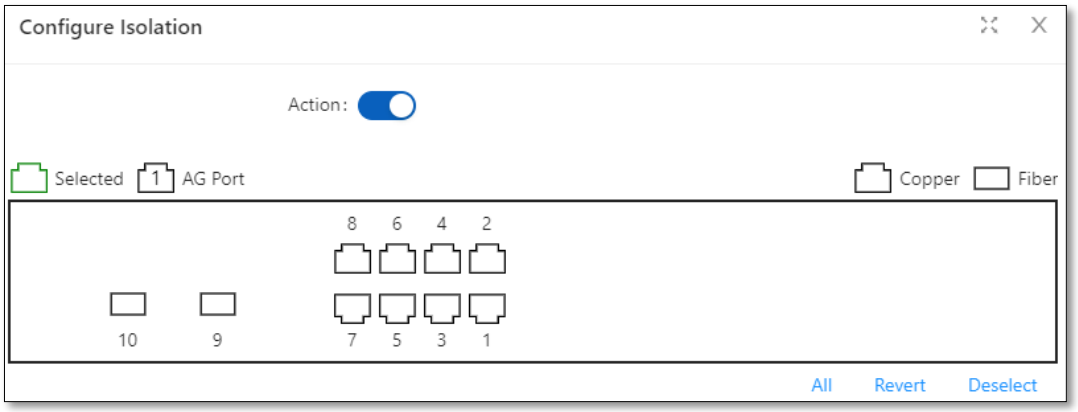


그림 3- 12 Isolation 설정

3.2.3 Port Mirroring

포트 미러링은 하나 이상의 포트(소스 인터페이스라고 함)를 통과하는 패킷을 로컬 장치의 포트(대상 인터페이스라고 함)로 복사하는 것입니다. 소스 인터페이스는 모니터링 장치와 연결됩니다. 모니터링 장치에서 대상 인터페이스로 미러링된 패킷을 분석하여 네트워크를 모니터링하고 가능한 네트워크 문제를 해결할 수 있습니다.

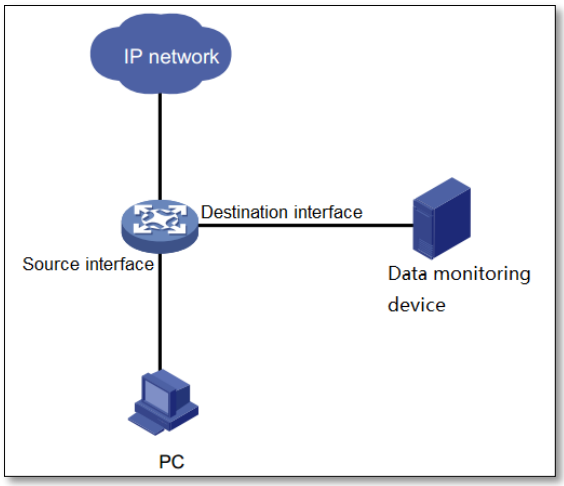


그림 3- 13 포트 미리링 구현

RSPAN(Remote Switch Port Analyzer)은 SPAN 의 확장입니다. 원격 미러 소스 포트와 대상 포트 사이에서 사용자는 여러 네트워크 장치를 스팬할 수 있습니다. RSPAN 의 원리는 원래 장치, 중간 장치 및 대상 장치가 세션에 참여하는 모든 포트가 추가되는 원격 VLAN 을 생성한다는 것입니다. 미러 메시지는 원격 VLAN 에서 브로드캐스트되어 그림 3-14 와 같이 소스 장치의 소스 포트에서 대상 장치의 대상 포트로 전송됩니다.

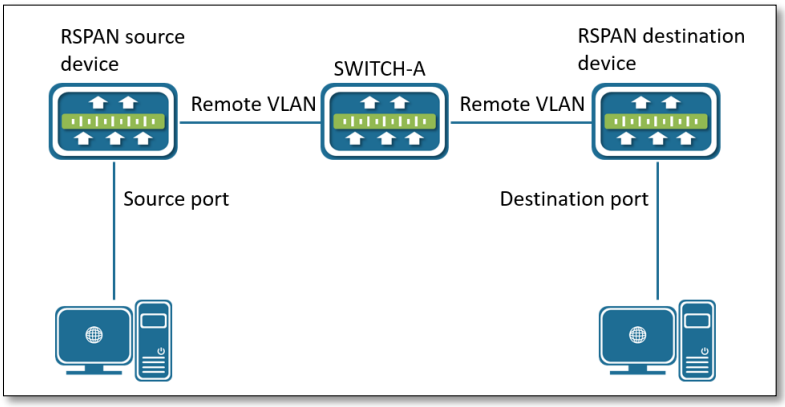


그림 3- 14 RSPAN

SPAN/RSPAN 은 소스 포트의 패킷 교환에는 영향을 미치지 않지만 소스 포트의 모든 입력 및 출력 패킷을 대상 포트에 복사할 뿐입니다. 예를 들어 소스 포트의 미러 트래픽이 대상 포트의

대역폭을 초과하면 100Mbps 대상 포트가 1000Mbps 소스 포트의 트래픽을 모니터링하여 메시지가 삭제될 수 있습니다.

사용자가 소스 포트와 대상 포트를 구성할 수 있는 세션 관리 기반 SPAN/RSPAN. 한 세션에서는 대상 포트가 하나만 있을 수 있지만 여러 소스 포트를 동시에 구성할 수 있습니다.

1. Configuration > Port > Port Mirror 메뉴에서 다음과 같이 포트 미러 페이지로 접속합니다.

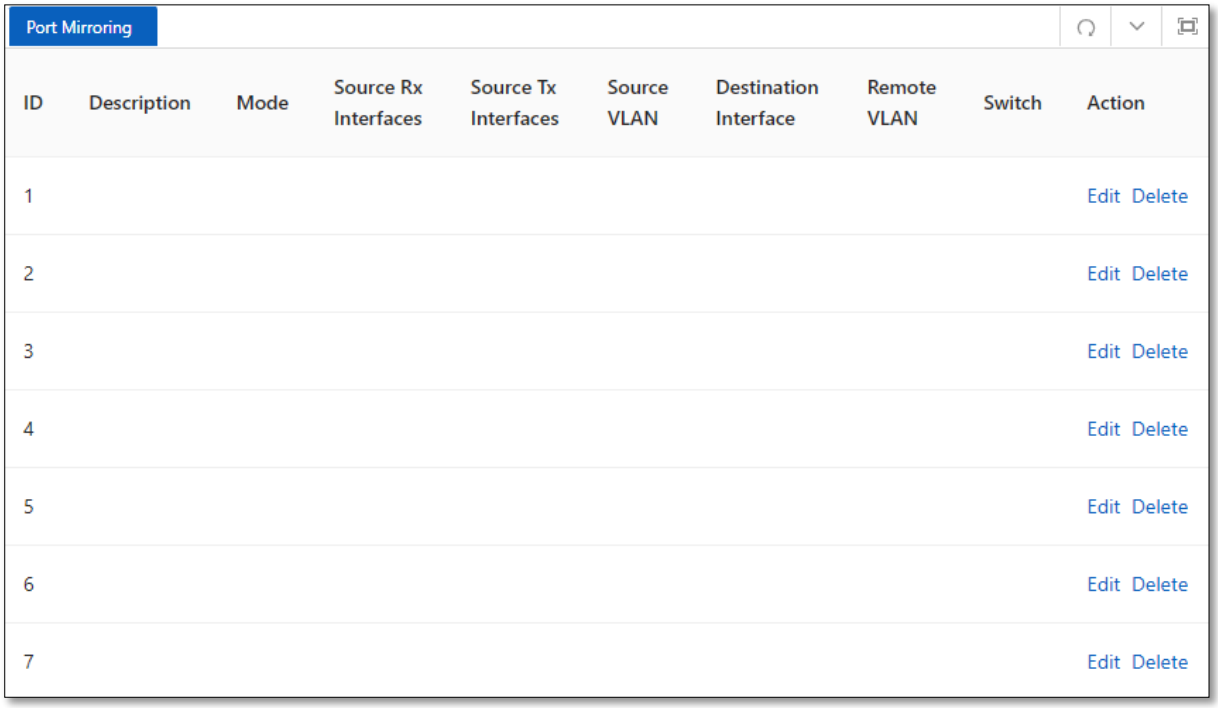


그림 3- 15 포트 미러링 설정

2. 해당 ID 에 대한 편집 버튼을 클릭하고 그림과 같이 대상 인터페이스 또는 소스 인터페이스를 선택합니다.

메뉴	설명
ID	생성할 미러링 그룹의 ID
설명	생성된 미러 그룹의 설명
모드	미러 그룹의 모드는 기본적으로 로컬 미러로 설정됩니다.
Source Rx Interfaces	미러 소스 RX 포트를 선택하여 여러 소스 RX 포트가 동시에 존재할 수 있도록 합니다.
Source Tx Interfaces	미러 소스 tx 포트를 선택하여 여러 소스 TX 포트가 동시에 존재할 수 있도록 합니다.
Source VLAN	범위 모드를 지원하는 SPAN 소스 VLAN 을 생성/삭제합니다. 소스 VLAN 은 하나의 세션만 지원할 수 있으며 소스 포트와 공존할 수 없습니다.

Destination Interfaces	미러링 대상 포트를 선택하고 세션당 하나의 대상 포트만 허용됩니다.
Switch	SPAN 의 목적지 포트가 교환에 관여하는지 여부
Remote VLAN	범위 모드를 지원하는 RSPAN 소스 VLAN 을 생성/삭제합니다. 소스 VLAN 은 하나의 세션만 지원할 수 있으며 소스 포트와 공존할 수 없습니다.

표 3- 7 미러링 그룹 생성 설정 메뉴

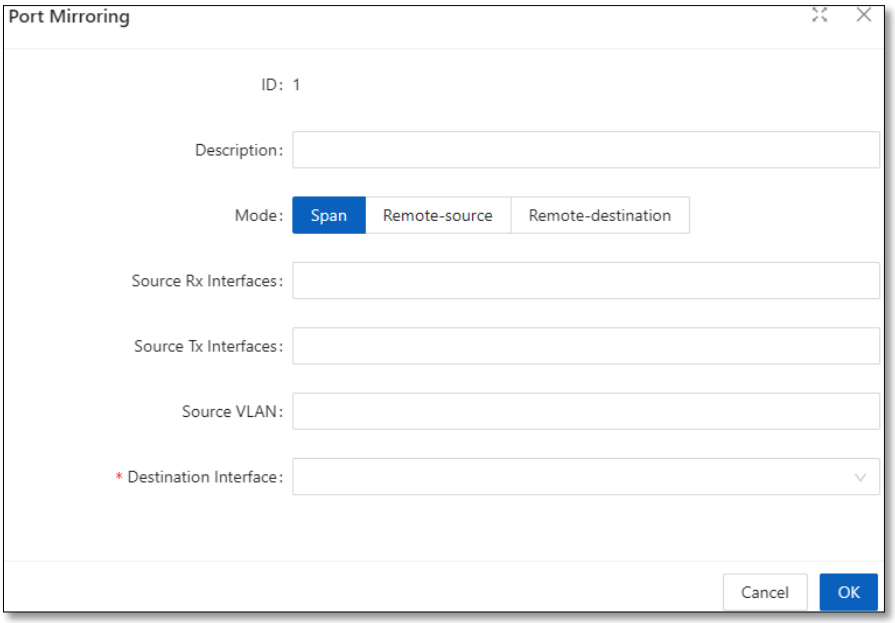


그림 3- 16 미러링 그룹생성

3. 요구 사항에 맞게 설정값을 입력하고 확인(OK) 버튼을 클릭하면 구성이 완료됩니다.

4. 설정 완료 후 저장하려면 저장버튼을 클릭합니다.

설정 예시

사례 요구 사항: 원격 장치 SWITCH-C 의 포트 gigabitEthernet0/8 을 사용하여 로컬 장치 SWITCH-A 의 포트 gigabitEthernet0/1 의 rx 메시지를 모니터링하고 원격 VLAN 은 1000 이며, 그동안 중간 장치는 VLAN 1000 메시지 브로드캐스트를 지원합니다. 이 모니터링 세션의 이름은 TRAFFIC_MONITOR_REMOTE 로 설정됩니다. 이러한 네트워크는 아래 그림 3-17 에 나와 있습니다.

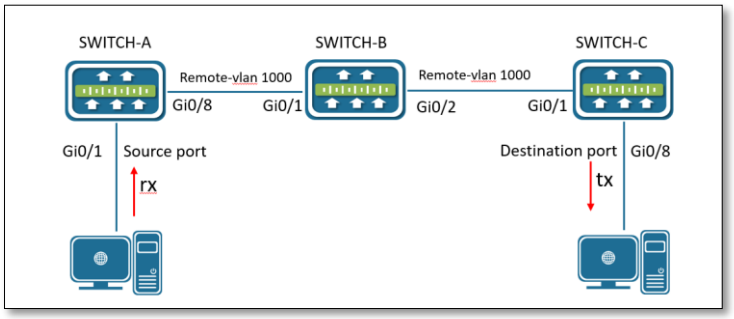


그림 3- 17 예시 토폴로지

스위치 A 구성:

1 단계: Configuration > Port > Port Mirroring 을 선택하여 포트 미러 페이지로 들어갑니다.

2 단계: 세션 1 에 해당하는 편집 버튼을 클릭하고 그림 3-18 과 같이 설정값을 입력한 다음 확인을 클릭합니다.

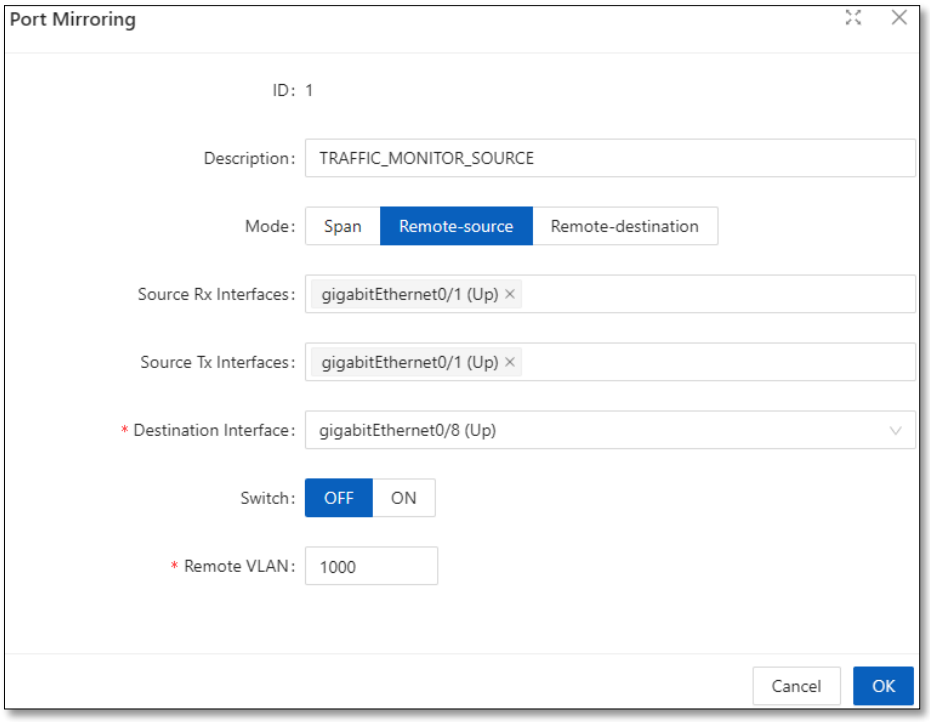


그림 3- 18 스위치 A 설정

3 단계: 보조 영역에서 Save 버튼을 클릭합니다.

스위치 B 구성:

1 단계: Configuration > VLAN 을 선택하여 VLAN Configuration 페이지로 들어갑니다.

2 단계: VLAN Configuration 아래의 +Add 버튼을 클릭하여 VLAN 이 1000 인 트렁크 포트로 gigabitEthernet0/1 과 gigabitEthernet0/2 를 구성합니다(그림 3-19 참조).

3 단계: 보조 영역에서 Save 버튼을 클릭합니다.

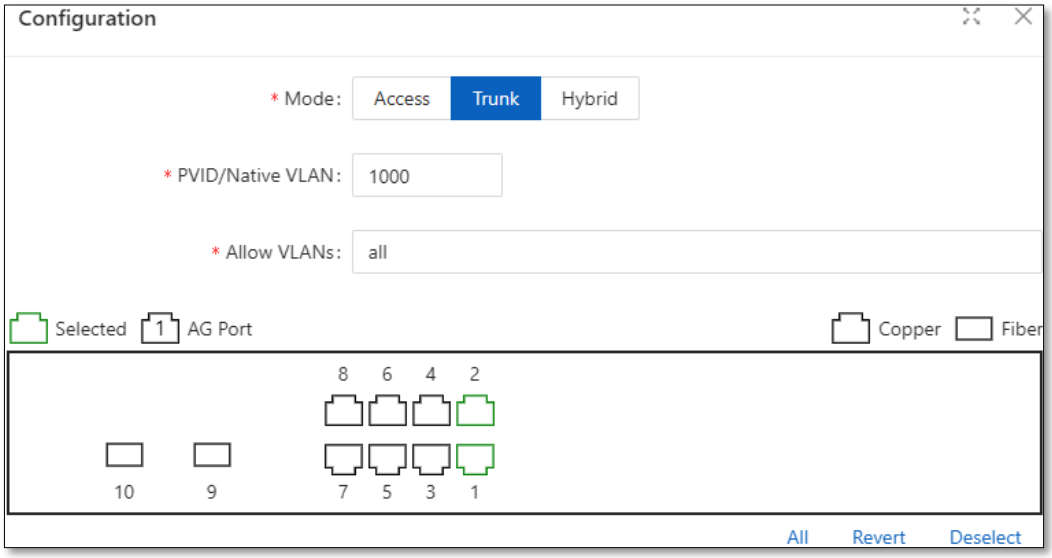


그림 3- 19 스위치 B 설정

스위치 C 구성:

1 단계: VLAN Configuration > VLAN 을 선택하여 VLAN 구성 페이지로 들어갑니다.

2 단계: VLAN 구성에서 +추가 버튼을 클릭하여 VLAN 1000 을 만듭니다.

3 단계: 그림 3-20 과 같이 gigabitEthernet0/8 을 액세스 포트로 구성하고 포트 VLAN 을 1000 으로 구성합니다.

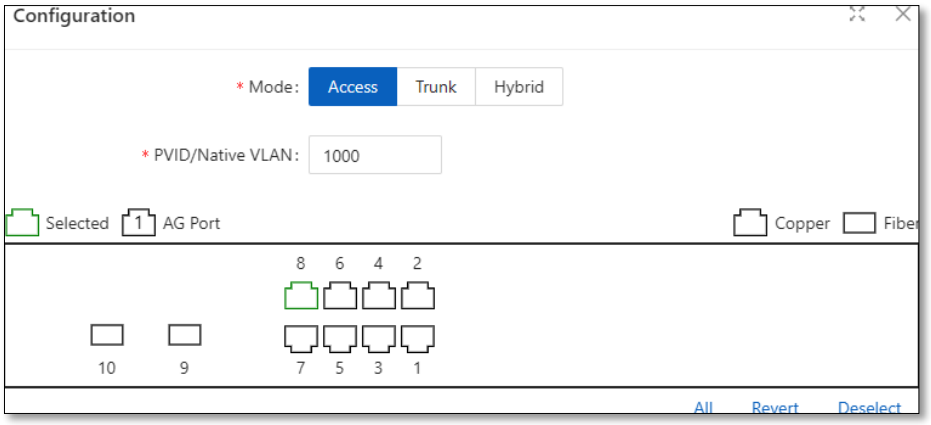


그림 3- 20 스위치 C 설정

4 단계: Configuration > Port > Port Mirroring 을 선택하여 Port Mirror 페이지로 들어갑니다.

5 단계: 세션 1 에 해당하는 Edit 버튼을 클릭하고 Figure 3-21 과 같이 매개변수를 입력한 다음 OK 를 클릭합니다.

6 단계: 보조 영역에서 Save 버튼을 클릭합니다.

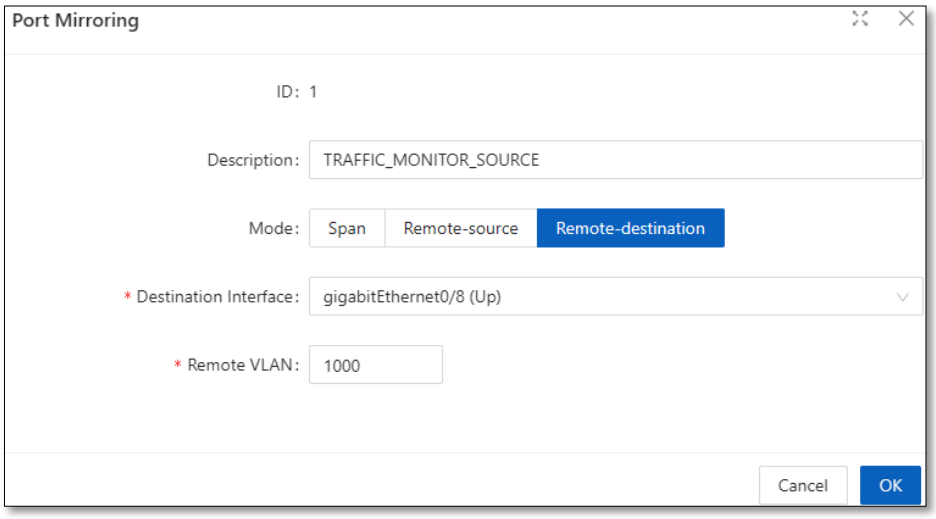


그림 3- 21 스위치 C 에서 미러링 설정

3.2.4 Port Aggregation

3.2.4.1 개요

Link Aggregation 이라고 불리는 이더넷 링크 통합은 여러 물리적 이더넷 링크를 하나의 논리적 링크로 통합하여 링크 대역폭을 단일 링크의 한계 이상으로 늘립니다. 물리적 링크가 서로 동적으로 백업되므로 링크의 중복성이 허용됩니다.

그림 3-16 처럼 스위치 A 와 스위치 B 는 3 개의 물리적 이더넷 링크로 연결됩니다. 이러한 물리적 이더넷 링크는 집합 링크인 링크 집합 1 로 집합됩니다. 이 집합 링크의 대역폭은 이 세 개의 물리적 이더넷 링크의 총 대역폭만큼 높을 수 있습니다.

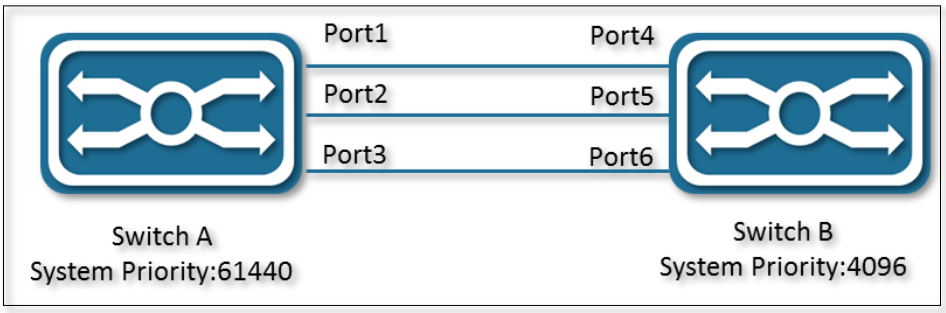


그림 3- 22 Link Aggregation

IEEE 802.3ad LACP(링크 집합 제어 프로토콜)는 물리적 링크의 동적 집합을 가능하게 합니다. LACP 를 지원하는 장치 간에 집합 정보를 교환하기 위해 LACPDU 를 사용합니다. LACP 는 동적 및 정적의 두 가지 모드가 있습니다. 동적 링크 통합은 LACP 를 사용하지만 정적 링크 통합은 LACP 를 사용하지 않습니다. 정적 모드로 동작하는 링크 집합 그룹을 정적 링크 집합 그룹, 동적 모드로 동작하는 링크 집합 그룹을 동적 링크 집합 그룹이라고 합니다.

3.2.4.2 Aggregation

1. Configuration > Port > Port Aggregation 메뉴에서 Link Aggregation 페이지로 접속합니다.

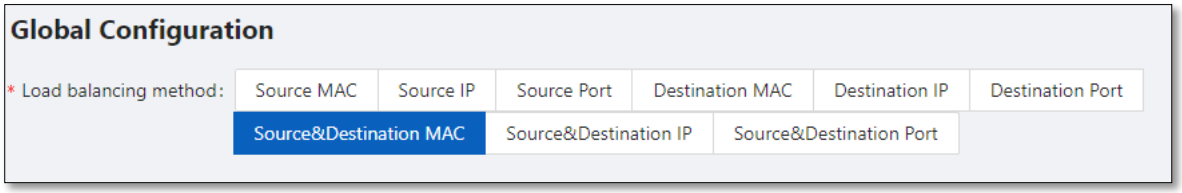


그림 3- 23 LACP 설정 페이지

메뉴	설명	
로드 밸런싱 방법	dst-mac	대상 MAC 주소에 따라 균등화
	src-mac	소스 MAC 주소에 따라 균등화
	src-dst-mac	대상 MAC 주소와 소스 MAC 주소에 따라 균등화
	dst-ip	대상 IP 주소에 따라 균등화
	srt-ip	소스 IP 주소에 따라 균등화
	src-dst-ip	대상 IP 주소와 소스 IP 주소에 따라 균등화
	dst-port	L4 TCP/UDP 대상 포트 번호에 따라 균등화
	src-port	L4 TCP/UDP 소스 포트 번호에 따라 균등화
	src-dst-port	L4 TCP/UDP 대상 포트 번호와 소스 포트 번호에 따라 균등화

표 3- 8 LACP 설정 메뉴 설명

2. LCAP 설정페이지에서 +추가 버튼을 클릭하여 그림과 같이 포트 설정 페이지로 접속합니다.

메뉴		설명	
포트 설정	ID	Aggregation 맴버 ID	
	유형	수동	수동 모드
		Active	이 모드에서 포트는 정기적으로 LACP 패킷을 보냅니다. 파트너 포트에 대한 간격
		Passive	이 모드에서는 포트가 LACP 패킷을 보내지 않습니다. 파트너 포트는 LACP 패킷을 보냅니다. 파트너 포트로부터 LACP 패킷을 수신한 후 포트는 LACP 패킷을 파트너 포트로 보냅니다.

표 3- 9 Aggregation 맴버 설명

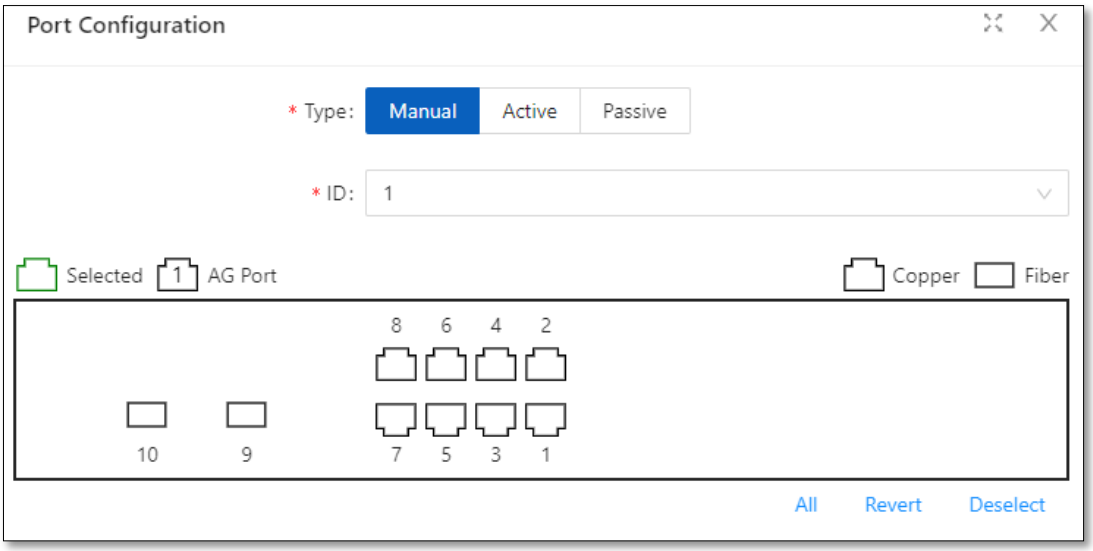


그림 3- 24 LACP 포트 설정

Type 을 선택하고 "ID" 상자에 텍스트를 입력한 후 포트 패널에서 포트를 선택하고 확인 버튼을 클릭하여 완료합니다.

설정이 완료되면 생성된 Aggregation Port 가 Aggregation Port 페이지에 다음과 같이 표시됩니다.



그림 3- 25 19 Aggregation 설명

메뉴		설명
Aggregation Port	ID	Aggregation ID
	Name	Aggregation 포트의 이름
	Type	Aggregation Port 모드
	Member	Aggregation Port 의 멤버 포트

표 3- 10 Aggregation 포트 설명

3.2.5 Port Violation

장치를 사용하는 동안 포트의 보안설정 위반, 포트 플래핑 위반, 포트 루프 감지 위반 등과 같은 경우가 스위치 포트에서 발생할 수 있습니다. 포트 위반 모듈은 복구 활성화 및 복구 시간을 설정하는 데 사용됩니다. 위반 포트를 표시하고 포트의 위반 동작을 표시합니다.

1. Configuration > Port > Port Violation 메뉴에서 Port Violation 설정 인터페이스로 접속합니다.

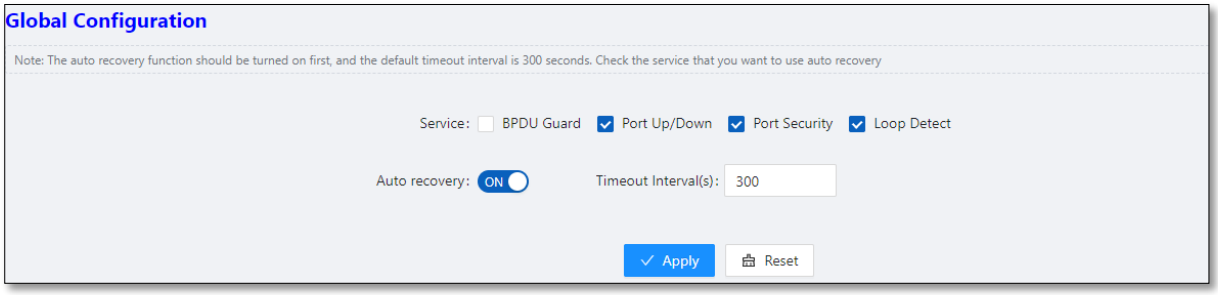


그림 3- 26 글로벌 설정 페이지

메뉴		설명
Service	BPDU Guard	포트 BPDU 보호로 인한 위반
	Port Up/Down	잦은 포트 Up/Down 으로 인한 위반
	Port Security	불법포트 보안으로 인한 위반
	Loop Detect	포트 다운스트림 장치의 루프로 인해 발생한 위반
Auto recovery		포트 자동 복구 활성화/비활성화
Timeout interval		포트의 복구 시간(초)을 구성합니다.

표 3- 11 글로벌 설정

Port Violation 을 수동으로 복원해야 하는 경우 복원해야 할 포트를 선택하고 Res(Res) 버튼을 클릭합니다. **Reset** 버튼을 클릭하면 포트 기능을 복원합니다

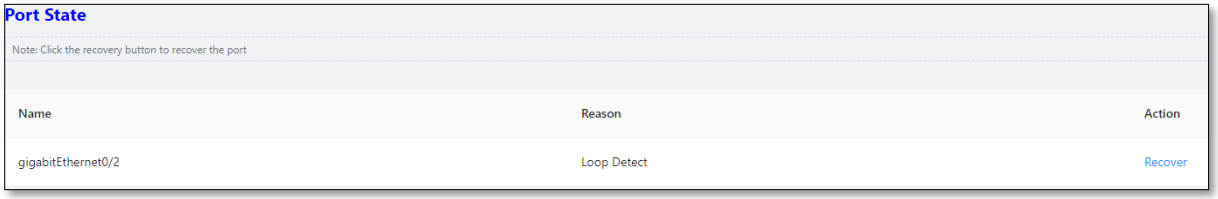


그림 3- 27 21 Port 상태

3.3 스패닝 트리

3.3.1 개요

STP(스패닝 트리 프로토콜)는 레이어 2 관리 프로토콜입니다. 레이어 2 루프를 제거하기 위해 중복 링크를 선택적으로 차단할 수 있을 뿐만 아니라 링크를 백업할 수도 있습니다. 많은 프로토콜과 마찬가지로 STP 는 네트워크가 발전함에 따라 RSTP(Rapid Spanning Tree Protocol)에서 MSTP(Multiple Spanning Tree Protocol)로 지속적으로 업데이트 되었습니다. 레이어 2 이더넷의 경우 두 개의 근거리 통신망(LAN) 사이에 하나의 활성 링크만 존재할 수 있습니다. 그렇지 않으면 브로드캐스트 충돌이 발생합니다. LAN 의 신뢰성을 높이려면 중복 링크를 설정하고 일부 경로를 백업 상태로 유지해야 합니다. 네트워크에 결함이 있고 링크에 장애가 발생하면 중복 링크를 활성 상태로 전환해야 합니다. STP 는 수동 작업 없이 자동으로 중복 링크를 활성화할 수 있습니다. STP 를 사용하면 LAN 의 장치에서 다음을 수행할 수 있습니다.

- LAN 에서 최고의 트리 토폴로지를 발견하고 복구합니다.
- 오류를 해결하고 가능한 최상의 트리 토폴로지가 항상 선택되도록 네트워크 토폴로지를 자동으로 업데이트합니다.

LAN 토폴로지는 관리자가 설정한 일련의 브리지 매개변수를 기반으로 자동으로 계산됩니다. 이러한 매개변수를 적절하게 설정하면 최상의 토폴로지 트리를 얻을 수 있습니다. RSTP 는 802.1D STP 와 완벽하게 호환됩니다. 기존 STP 와 마찬가지로 RSTP 는 루프 없는 중복 서비스를 제공합니다. 복구 속도가 빠른 것이 특징입니다. LAN 의 모든 브리지가 RSTP 를 지원하고 관리자가 적절하게 설정한 경우 네트워크 토폴로지가 변경된 후 토폴로지 트리를 다시 생성하는 데 1 초 미만이 걸립니다.

STP 와 RSTP 에는 다음과 같은 결함이 있습니다.

STP 마이그레이션이 느립니다. 지점 간 링크 또는 에지 포트에서도 포트가 전달 상태로 전환되는 데 여전히 전달 지연의 2 배가 걸립니다. RSTP 는 빠르게 수렴할 수 있지만 STP 와 동일한 결함이 있습니다. LAN 의 모든 VLAN 이 동일한 스패닝 트리를 공유하므로 모든 VLAN 의 패킷이 이 스패닝 트리를 따라 전달됩니다. 따라서 특정 VLAN 에 따라 중복 링크를 차단할 수 없으며 VLAN 간에 데이터 트래픽의 균형을 맞출 수 없습니다. IEEE 가 802.1s 에서 정의한 MSTP 는 STP 와 RSTP 의 결함을 해결합니다. 이는 신속하게 수렴할 수 있을 뿐만 아니라 서로 다른 VLAN 의 트래픽이 각 경로를 따라 전달되도록 할 수 있으므로 중복 링크에 대해 더 나은 로드 밸런싱 메커니즘을 제공합니다. 일반적으로 STP/RSTP 는 포트를 기반으로 동작하지만 MSTP 는

인스턴스를 기반으로 동작합니다. 인스턴스는 여러 VLAN 의 집합입니다. 여러 VLAN 을 하나의 인스턴스에 바인딩하면 통신 오버헤드와 리소스 활용도를 줄일 수 있습니다.

3.3.2 스패닝 트리 설정

1. Configuration > Spanning Tree > Global Configuration 메뉴에서 Global Configuration 설정 페이지로 접속합니다.

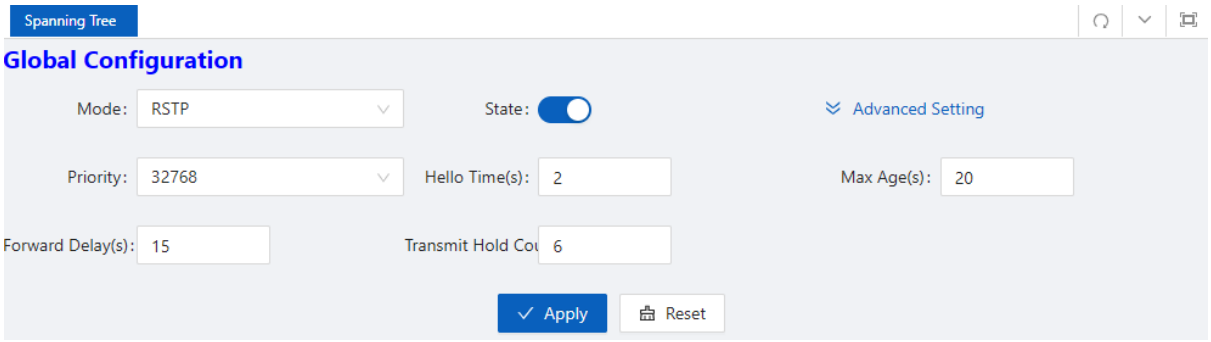


그림 3- 28 스패닝 트리

메뉴		설명
글로벌 설정	방법	STP, RSTP 및 MSTP 를 포함하여 STP 의 동작 모드를 설정합니다. STP: STP 모드에서는 장치의 각 포트가 STP BPDU 를 보냅니다. RSTP: RSTP 모드에서는 장치의 각 포트가 RSTP BPDU 를전송합니다. STP 를 실행하는 장치에 연결되면 포트가 자동으로 STP 모드로 마이그레이션됩니다. MSTP: MSTP 모드에서는 장치의 각 포트가 MSTP BPDU 를 보냅니다. STP 를 실행하는 장치에 연결되면 포트는 STP 모드에서 동작하도록 자동으로 마이그레이션됩니다.
	상태	STP 를 활성화합니다.
	Hello 시간	Hello 타이머 간격
	우선 사항	브리지 우선순위
	전달 지연	인터페이스가 전달로 변경되기 전 지연 시간을 설정합니다.
	전송 보류 횟수	브리지에서 초당 전송하는 최대 BPDU 수
	Max age	메시지가 장치에 저장되는 최대 기간 설정

표 3- 12 스패닝 트리 설정 메뉴

2. Configuration > Spanning Tree > Instance Configuration 메뉴에서 instance configuration 으로 접속합니다.

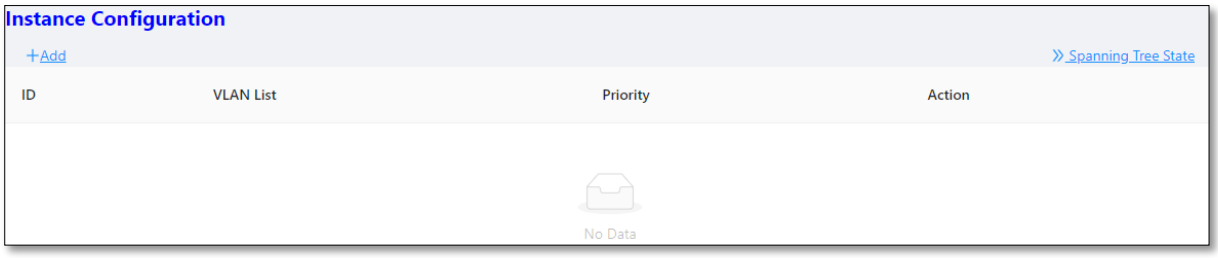


그림 3- 29 스패닝 트리 인스턴스 설정

메뉴		설명
Instance Configuration	ID	인스턴스 ID
	VLAN List	인스턴스 관련 VLAN 목록
	Priority	이 경우 브리지 우선순위
	Action	이 메뉴를 삭제하려면 클릭하세요.

표 3- 13 스패닝 트리 인스턴스 메뉴

3. Configuration > Spanning Tree > Port Configuration 메뉴에서 port configuration 설정 화면으로 접속합니다.

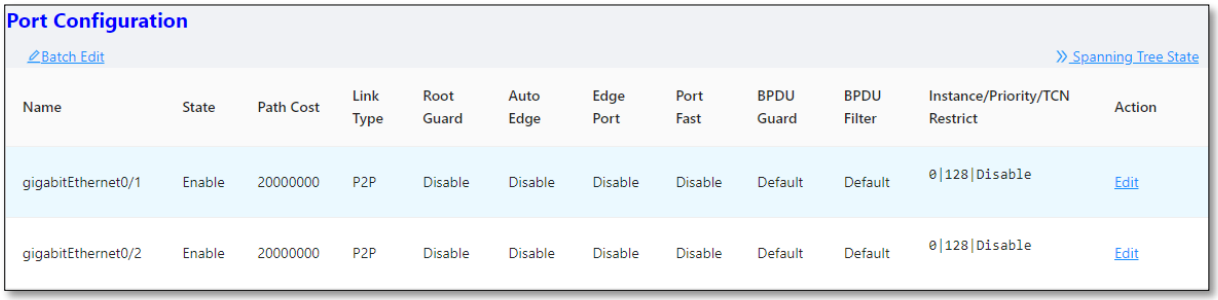


그림 3- 30 스패닝 트리 포트 설정

메뉴		설명
Port Configuration	Name	인터페이스 이름
	State	STP 상태
	Path Cost	인터페이스 경로 비용 설정
	Link Type	인터페이스 링크 유형 설정
	Root Guard	루트 보호를 활성화하도록 인터페이스를 설정합니다.
	Auto Edge	Edge 포트의 기능을 자동으로 인식하도록 인터페이스를 설정합니다.
	Edge Port	인터페이스를 엣지 포트로 설정합니다.
	Port Fast	인터페이스를 고속 포트로 설정하십시오.
	BPDU Filter	BPDU 필터링을 활성화하도록 인터페이스를 설정합니다.
	BPDU Guard	BPDU 보호를 활성화하도록 인터페이스를 설정합니다.
	Instance/Priority/TCN restrict	설정이자형 사례, 우선순위 및 TCN 제한.

표 3- 14 스패닝 트리 포트 설정 메뉴

3.4 ERPS

3.4.1 개요

ITU-T G.8032 ERPS 기능은 이더넷 레이어 링 토폴로지에 대한 보호 전환 메커니즘을 구현합니다. 이 기능은 ITU-T G.8032 에 정의된 G.8032 이더넷 링 보호(ERP) 프로토콜을 사용하여 링 토폴로지의 이더넷 트래픽에 대한 보호를 제공하는 동시에 이더넷 계층의 링 내에 루프가 없도록 보장합니다. 미리 결정된 링크나 실패한 링크의 트래픽을 차단하여 루프를 방지합니다.

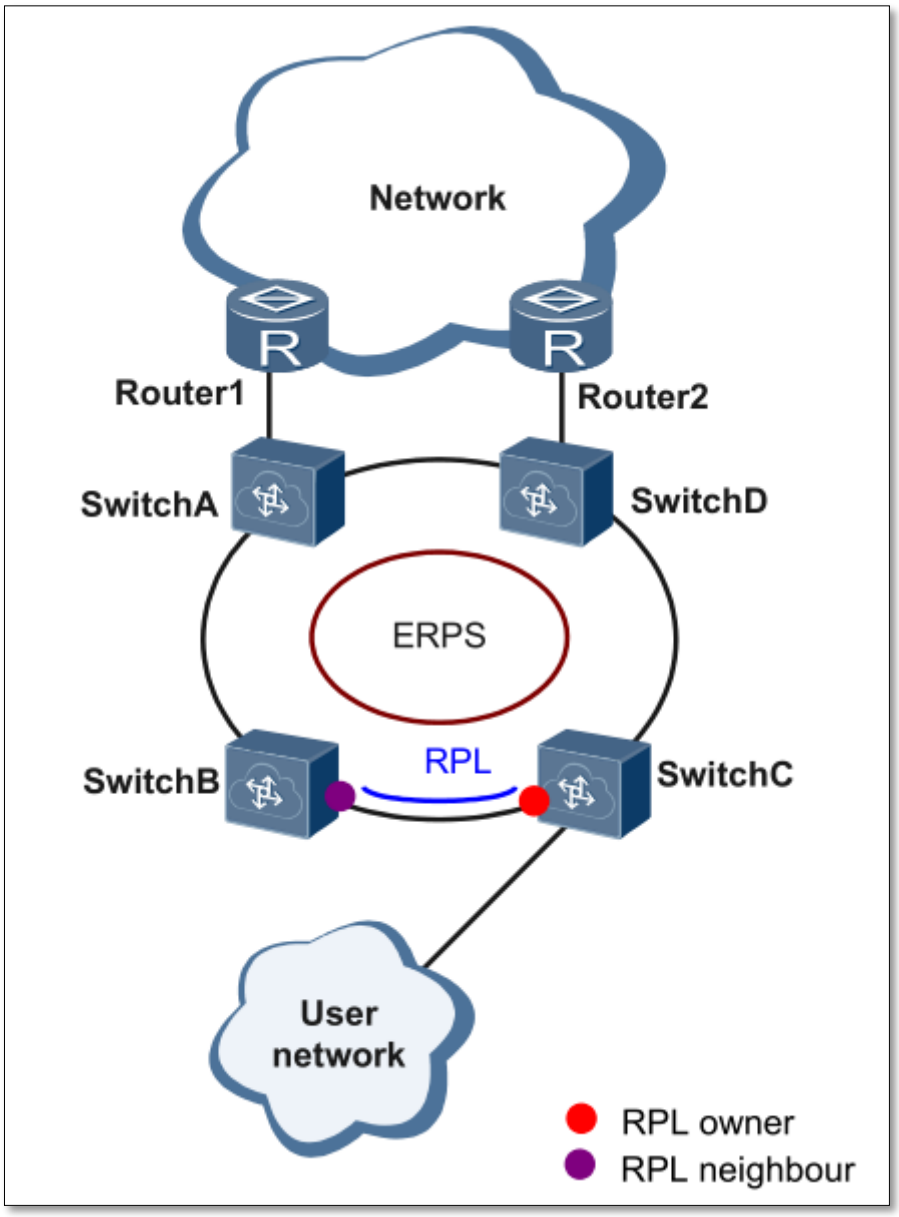


그림 3- 31 ERPS 초기 상태

- 초기 상태

다음 그림과 같이 링의 장치가 설정되었으며 모든 링크 상태가 Up 입니다.

RPL owner 인터페이스는 루프를 방지하기 위해 ERPS 프로토콜에 의해 차단됩니다. RPL 인접 인터페이스가 설정된 경우 해당 인터페이스도 차단됩니다. 다른 인터페이스는 전달 상태에 있으므로 트래픽을 전달할 수 있습니다.

- 링크 실패

SwitchD 와 SwitchE 사이에 링크 오류가 발생하면 링크의 두 인터페이스가 ERPS 프로토콜에 의해 차단되고 RPL owner 인터페이스가 전달됩니다.

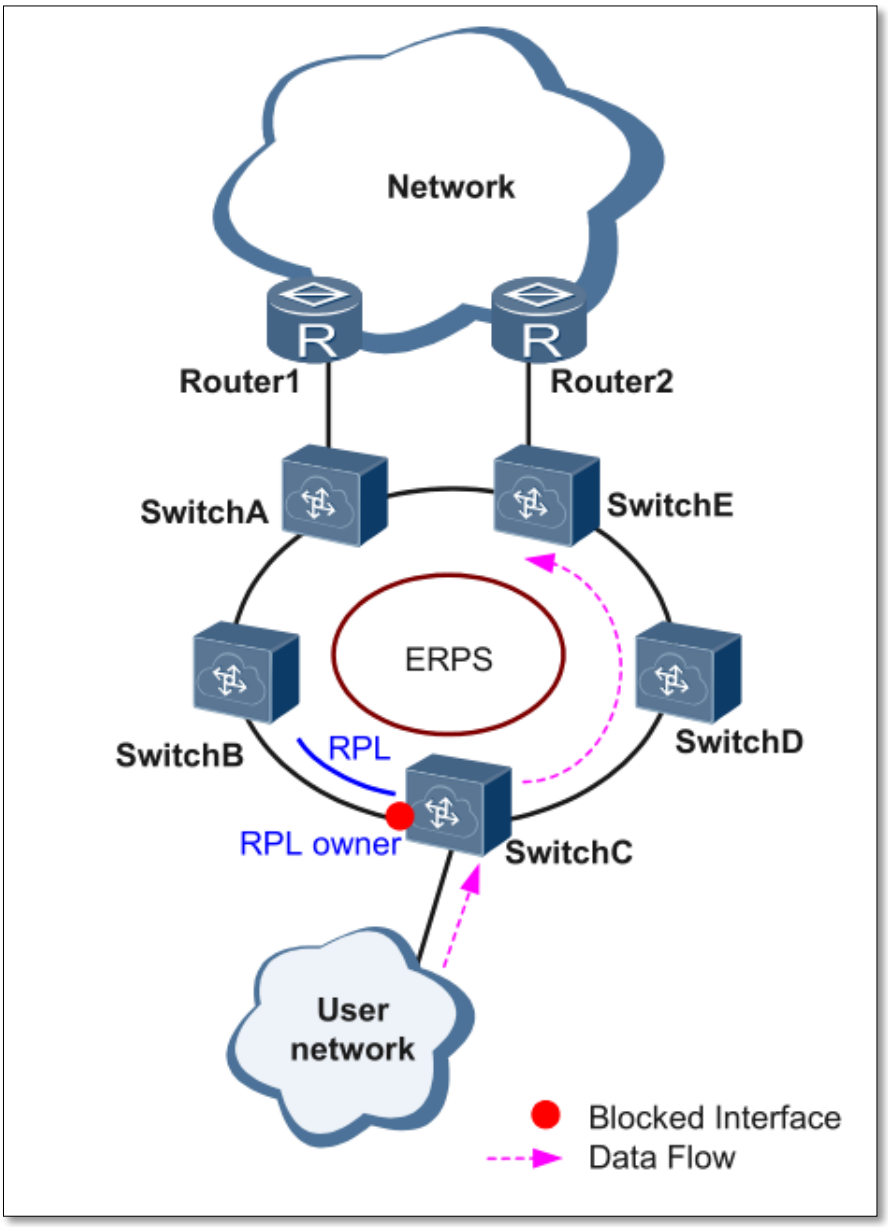


그림 3- 32 링크 실패 시 동작

- 링크 복원

장애 링크가 복원된 경우. erps 링이 복귀 모드로 설정되면 RPL owner 인터페이스가 ERPS 프로토콜에 의해 차단되고 복원된 링크는 트래픽을 전달하기 위한 전달 상태로 설정됩니다.

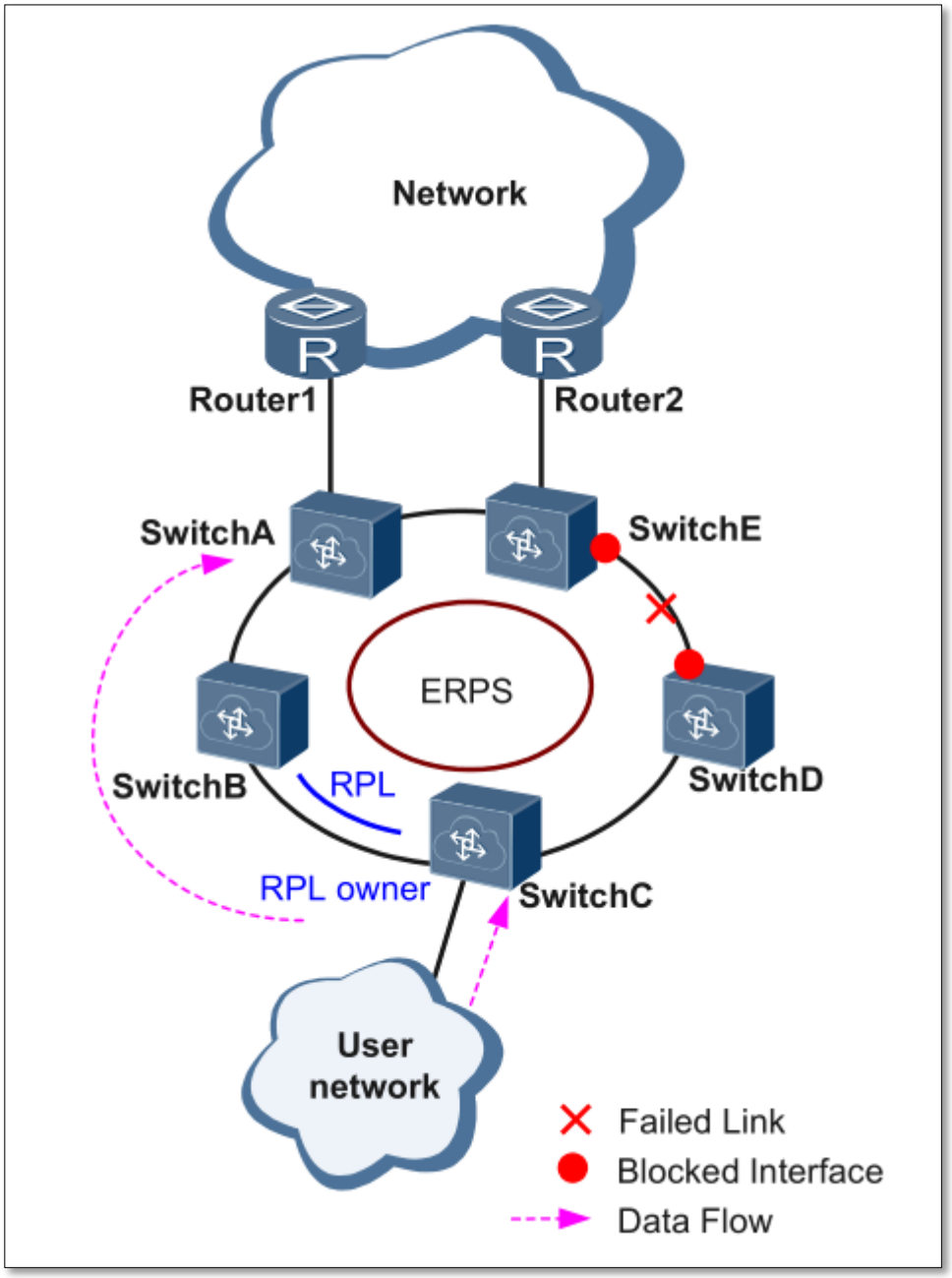


그림 3- 33 링크 복원

- Single Ring

네트워크 토폴로지에서 하나의 링만 보호하면 됩니다

네트워크 토폴로지에는 링 1 개, RPL(링 보호 링크) owner 노드 1 개, RPL 1 개만 있습니다. 모든 노드는 동일한 R-APS(링 자동 보호 스위칭) VLAN(가상 근거리 통신망)에 속해야 합니다.

- 링네트워크의 모든 장치는 ERPS 를 지원해야 합니다.
- 링 네트워크의 장치 간 링크는 직접 연결되어야 하며 중간 장치가 없어야 합니다.

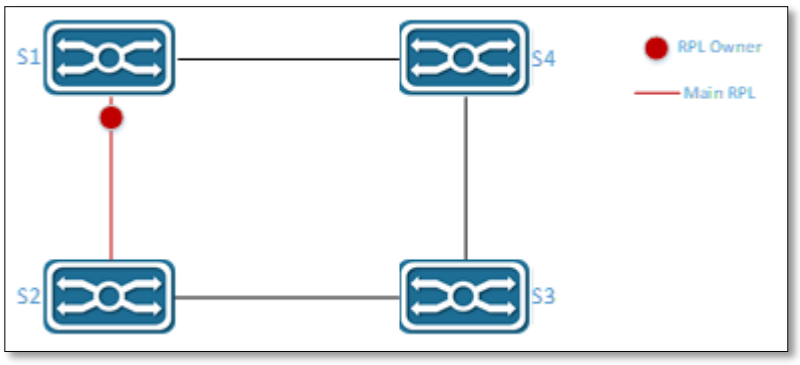


그림 3- 34 Single Ring ERPS

- Tangent Ring

하나의 장치를 공유하는 네트워크 토폴로지의 두 링은 보호되어야 합니다.

- 링 네트워크의 모든 장치는 ERPS 를 지원해야 합니다.
- 링 네트워크의 장치 간 링크는 직접 연결되어야 하며 중간 장치가 없어야 합니다.

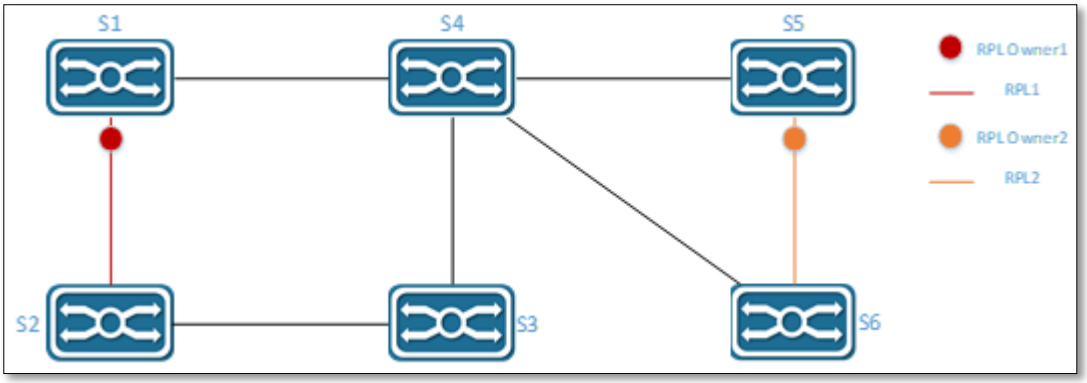


그림 3- 35 Tangent Ring ERPS

- Intersceting Ring

네트워크 토폴로지에 두 개 이상의 링은 하나의 링크를 공유합니다. (교차하는 노드 사이의 각 링크는 중간 노드가 없는 직접 링크여야 합니다.)

네트워크 토폴로지에 4 개의 링이 존재합니다. 각 링에는 단 하나의 PRL owner 노드와 단 하나의 RPL 만 있습니다. 4 개의 링은 서로 다른 R-APS VLAN 에 속합니다.

- 링 네트워크의 모든 장치는 ERPS 를 지원해야 합니다.
- 링 네트워크의 장치 간 링크는 직접 연결되어야 하며 중간 장치가 없어야 합니다.

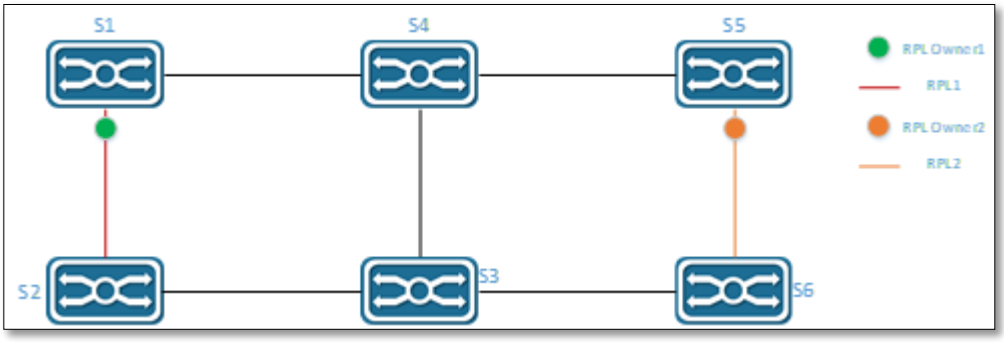


그림 3- 36 Intersecting Ring ERPS

1. Configuration > ERPS > Instance Configuration 메뉴에서 ERPS instance configuration 페이지로 접속합니다.

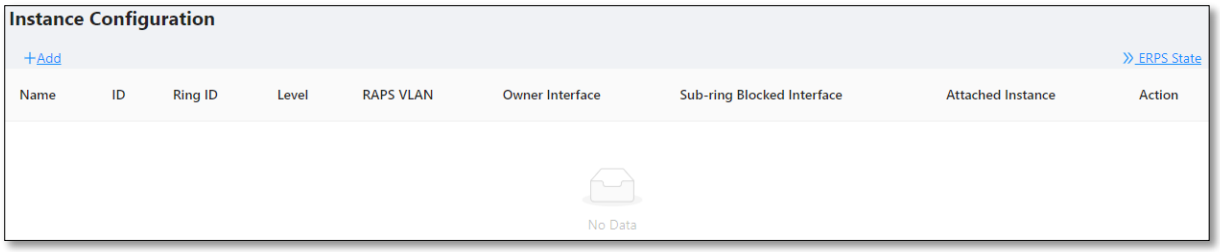


그림 3- 37 ERPS 링 설정

메뉴	설명
Ring ID	임의의 숫자가 될 수 있습니다. 각 ERPS 링의 링 번호는 고유해야 합니다.
East Interface	ERPS 링의 East 인터페이스
West Interface	ERPS 링의 West 인터페이스
Action	ERPS 링 삭제

표 3- 15 ERPS 인스턴스 설정

2. Configuration > ERPS > Instance Configuration 메뉴에서 ERPS instance 페이지로 접속합니다.

메뉴	설명
Ring Configuration	새로 생성하거나 생성된 ERPS 링에 연결
Ring ID	연결된 링 ID 는 생성된 링이어야 합니다.
East Interface	ERPS 링의 East 인터페이스
West Interface	ERPS 링의 West 인터페이스
RAPS VLAN	동일한 링에 있는 각 스위치는 ERPS 프로토콜 패킷 전송을 위해 동일한 RAPS 관리 VLAN 으로 설정되어야 합니다. RAPS 관리 VLAN 은 가상 VLAN 일 수 있으며 데이터 VLAN 과 구별되어야 합니다.
Owner interface	ERPS owner 인터페이스는 동쪽 인터페이스 또는 서쪽 인터페이스를 선택할 수 있습니다. Owner 노드 인터페이스 각 ERPS 링에는 차단해야 하는 포트를 제어하는 RPL 소유자 인터페이스로 설정된 단 하나의 인터페이스가 있습니다.
Sub-ring Block Interface	하위 링의 차단된 인터페이스, 하나의 하위 링에는 차단 포트가 하나만 있습니다. 동쪽이나 서쪽을 선택할 수 있습니다. 이 매개변수는 접선 링에 대해서만 설정해야 합니다. 링에 접하는 두 장치의 서브 링은 서브 링 차단 포트로 설정되어야 합니다.
Ring Configuration	서브링 차단 포트를 설정해야 하는 경우에만 설정하면 되며, 현재 서브링과 접하는 링 ID 로 설정됩니다.
Attached Instance	서브 링 차단 포트를 구성해야 하는 경우에만 설정하면 되며, 현재 서브 링에 접하는 링 ID 로 설정됩니다.

표 3- 16 ERPS Instance 설정

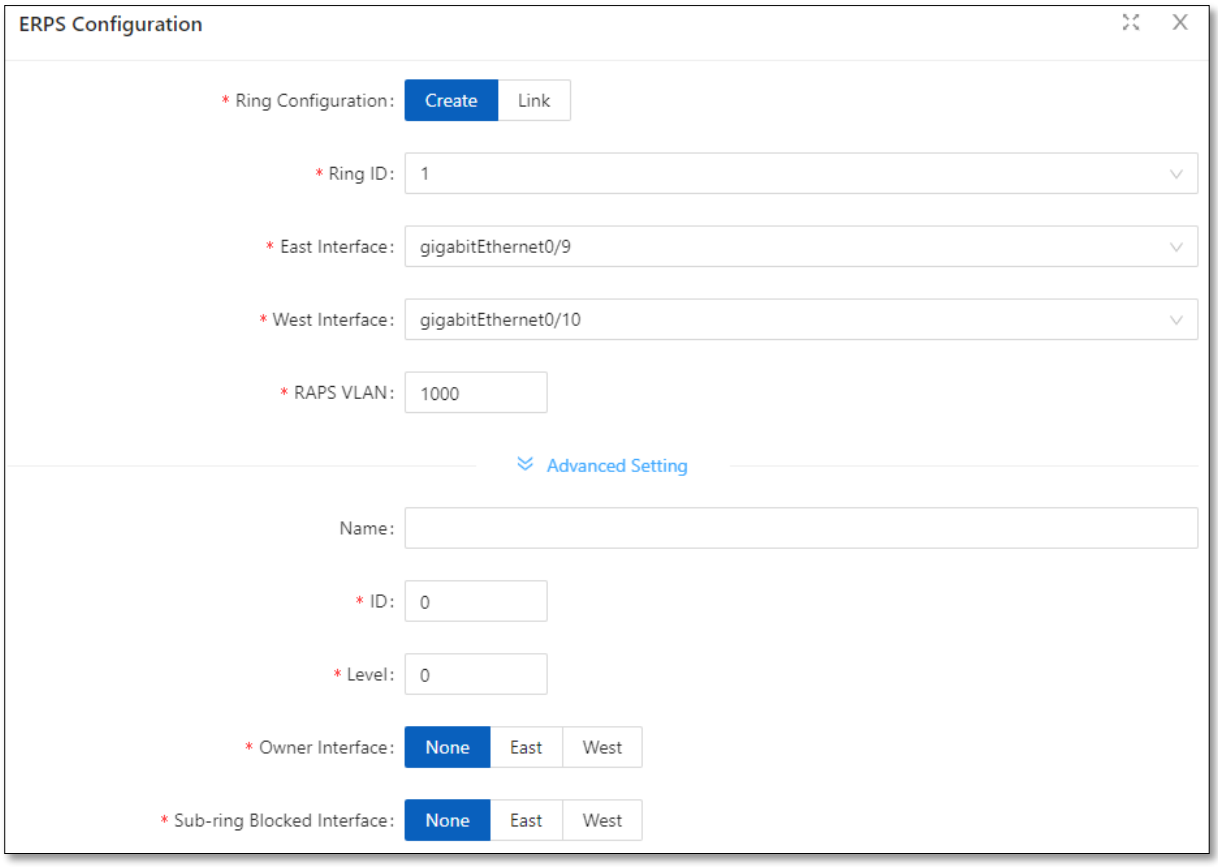


그림 3- 38 ERPS Instance 설정

3. ERPS State 를 클릭하여 ERPS State 페이지로 접속합니다.

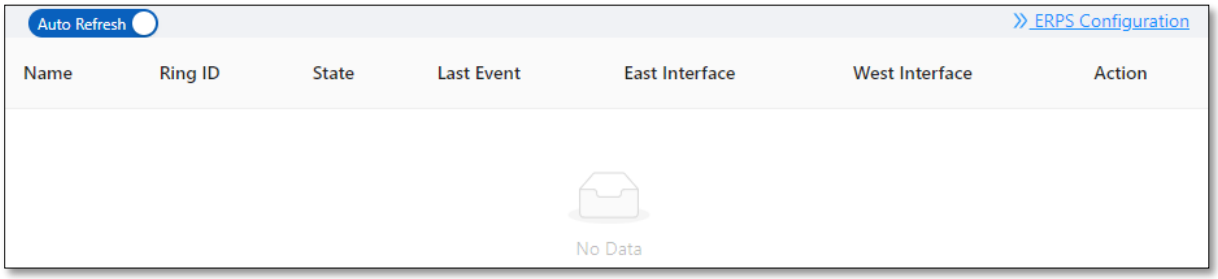


그림 3- 39 ERPS 상태보기

메뉴	설명
Name	ERPS 링의 이름
Ring ID	ERPS 링의 수
State	ERPS 링 상태,포함하다: 게으른:

	RPL 이 아닌 모든 링크를 사용할 수 있는 안정적인 상태입니다. 이 상태에서 owner 노드는 RPL 포트를 차단하고 주기적으로 NR-RB 패킷을 보냅니다. 인접 노드가 RPL 포트를 차단합니다. owner 노드가 유휴 상태에 들어간 후에 모든 노드는 유휴 상태에 들어갑니다. 보류 중: 이전 상태 사이의 과도 상태 보호: 비 RPL 링크에 결함이 있는 경우의 상태입니다. 이 상태에서는 트래픽 전달을 위해 RPL 링크가 차단 해제됩니다. 노드가 보호 상태에 들어간 후에 모든 노드는 보호 상태에 들어갑니다.
Last Event	최근 주 이벤트 RAPS -NR: 원격 장애 복구 RAPS -NR-RB: 원격 스위치백 RAPS-SF: 원격 오류 LOCAL-SF: 로컬 오류 LOCAL-CLEAR-SF: 로컬 장애 복구 WTR-EXP: 로컬 스위치백
East Interface	ERPS 링의 east 인터페이스
West Interface	ERPS 링의 west 인터페이스
Action	결함이 있는 링크가 복원되면 즉시 수동으로 되돌리도록 선택할 수 있습니다. 그렇지 않으면 시스템이 5 분 후에 자동으로 되돌려집니다.

표 3- 17 ERPS State 설명

3.5 PoE Management

3.5.1 개요

PoE(Power over Ethernet)는 PSE(Power Sourcing Equipment)가 케이블을 통해 이더넷 인터페이스에서 PD(Powered Device)에 전원을 공급하는 것을 의미합니다.

3.5.2 PoE Configuration

NOTE:

- PoE 를 설정하기 전에 PoE 전원 공급 장치와 PSE 가 정상적으로 동작하는지 확인하십시오. 그렇지 않으면 PoE 를 설정할 수 없거나 설정된 PoE 기능이 적용되지 않습니다.
- 외부 전원을 사용하는 스위치의 경우 입력 전압 범위는 44~57V 입니다. 보다 안정적인 전원 공급을 위해서는 AT 장비의 전원 전압은 50V 이상, BT 장비의 전원 전압은 50V 이상을 권장합니다.

1. Configuration > PoE 메뉴에서 PoE Management 페이지로 접속합니다.
2. "Power supply" 및 "Power reserved" 빈칸을 입력하고 적용 버튼을 클릭합니다.

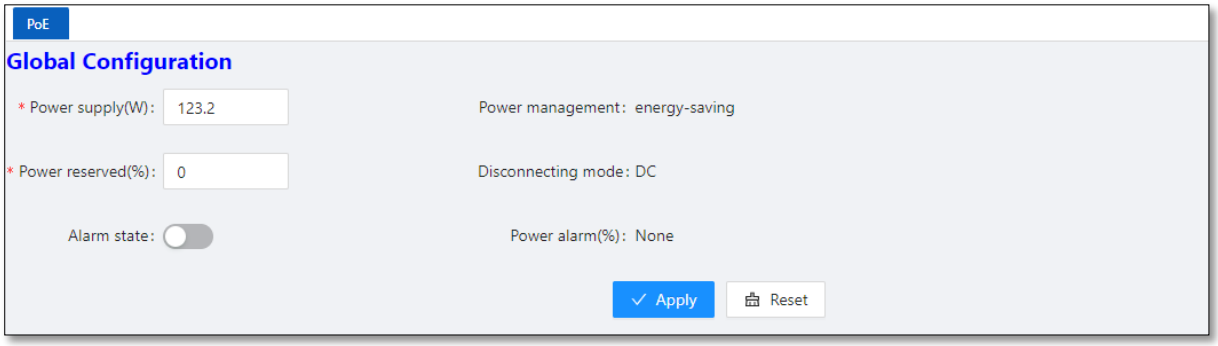


그림 3- 40 PoE Global 설정

메뉴	설명
Power supply (w)	기본적으로 장치가 제공하는 기본 전력은 15.4W*포트 수입니다. 예를 들어 8 포트 장치가 제공하는 최대 전력은 123.2W 입니다. •외부 전원 공급 장치가 있는 장치의 경우 실제 설정된 전원 공급 장치에 따라 이 설정 값을 입력하십시오. • 내장형 전원 공급 장치가 있는 장치의 경우 이 매개변수에 대한 제품 설명서의 PoE 전원 설명을 참조하세요.

Power reserved (%)	전력 변동에 대비한 예비 전력 설정 • 외부 전원 공급 장치가 있는 장치의 경우 메인 보드의 전력 소비를 채우는 것이 좋습니다. • 내장형 전원 공급 장치가 있는 장치의 경우 이 설정 값은 기본적으로 0 으로 설정
Power management	전원 관리 모드가 에너지 절약임을 표시합니다. 이 모드에서 포트에 요청되고 할당되는 전력은 실제 포트의 (실시간) 전력 소비를 기반으로 합니다.
Disconnect mode	연결 해제 모드가 DC 연결 해제임을 표시합니다.
Alarm state	전력이 부족할 때 로그 알람 켜기/끄기
Power alarm (%)	경보전력 제한설정 이 값을 초과하면 시스템이 자동으로 로그 알람을 출력합니다.

표 3- 18 PoE Global 설정

3. "port configuration" 메뉴에서 PoE port configuration page 로 접속하여 설정할 포트를 선택합니다.

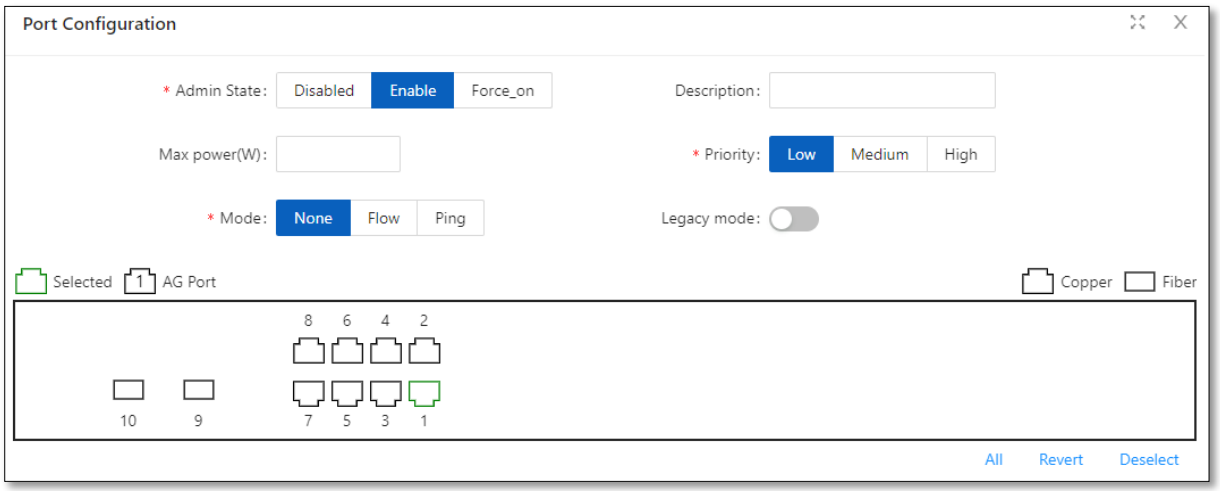


그림 3- 41 인터페이스 설정

4. 확인을 클릭하여 작업을 완료하면 다음과 같은 페이지가 PoE 인터페이스 설정 페이지로 접속합니다.

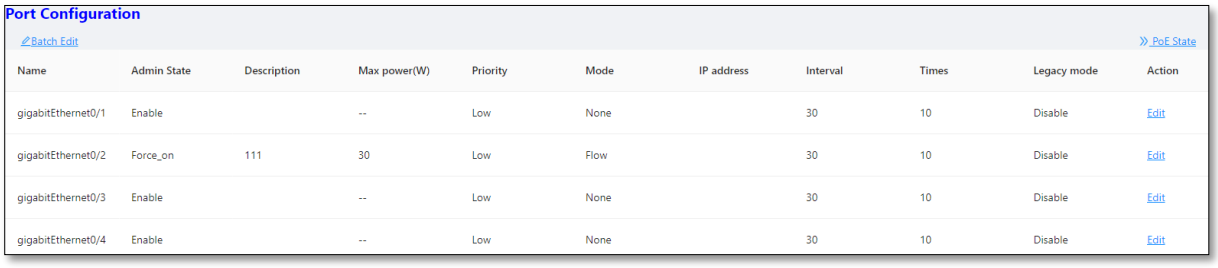


그림 3- 42 PoE 인터페이스 설정

5. 설정을 저장하려면 저장을 클릭합니다.

메뉴	설명
Name	표시 패널 포트 번호
Admin State	PoE 인터페이스에 대해 PoE 를 활성화/비활성화합니다. 비활성화됨: 포트의 PoE 전원 공급 장치를 비활성화합니다. 활성화: 포트의 Po E 전원 공급 장치를 활성화합니다. Force_on: 포트의 PoE 전원 공급 장치를 강제로 켭니다. PD 유효 검출과 PD 분류 검출을 건너뛰고 직접 공급합니다. PD 부하에 전원을 공급합니다. 이 모드에서 필요한 경우 기본 최대 부하 전력은 15w 입니다. 15W 이상으로 장치에 전력을 공급하려면 최대 전력을 설정해야 합니다.
Description	PoE 포트 설명
Max Power (W)	이 포트의 최대 전력을 설정합니다. AF/AT 포트의 경우 최대 포트 전력 범위는 1-30 입니다. BT 포트의 경우 포트 최대 전력 범위는 1-90 입니다. 기본 모드에서 포트는 PD 클래스에 따라 전원 관리를 수행합니다.
Priority	포트 우선순위 설정 사용자는 PoE 스위치의 인터페이스 전원 공급 우선순위를 설정할 수 있습니다. 우선순위는 높음부터 낮음, 높음, 중간, 낮음입니다. PoE 스위치의 전체 전력이 부족하면 우선 순위가 낮은 포트의 전원이 먼저 꺼집니다. 동일한 우선순위의 포트 우선순위는 포트 번호 순서대로 정렬되며, 포트 번호가 작은 포트의 우선순위가 높습니다. 예를 들어 포트 0/1 의 우선순위는 포트 0/2 및 0/3 보다 높습니다. 새로 설정된 포트는 이미 전원이 공급되고 우선순위가 동일한 PD 의 전원 공급 장치에 영향을 미치지 않습니다. 우선순위가 더 높은 새로 삽입된 포트는 우선순위가 낮은 포트를 선점합니다.
Mode	없음: PD 활성 감지 기능을 비활성화합니다.

	흐름: 흐름 모드에서 PD 감지 기능을 활성화합니다. 이 기능은 포트 카운터를 모니터링하여 구현되며, 포트 패킷 카운터가 변경되지 않으면 포트에 연결된 PD 장치가 비정상 상태라고 판단한 후 몇 초 동안 전원 공급 장치를 껐다가 다시 켜십시오. Ping: Ping 모드에서 PD 활성 감지 기능을 활성화합니다. 이 기능은 PD 부하에 대해 지속적으로 ping 을 함으로써 구현되며, 해당 간격 동안 ping 패킷이 일정 시간 실패하면 해당 포트에 연결된 PD 장치의 상태가 비정상이라고 판단하여 전원 공급이 잠시 차단된 후 몇 초 후에 다시 켜집니다. 스위치 진단 네트워크 도구를 사용하는 것이 좋습니다.→이 기능을 활성화하기 전에 PD 장치의 핑 패킷을 사용할 수 있는지 여부를 테스트하기 위해 ping 을 수행합니다.
IP address	Ping 모드에서는 PD 로드의 IP 주소를 사용하려면 스위치와 PD 로드가 동일한 네트워크 세그먼트에 있어야 합니다.
Interval	감지 시간 간격
Times	탐지 시간 PD 시작 시간은 간격 * 횟수보다 작아야 합니다. 그렇지 않으면 PD 로드는 항상 전원이 꺼지고 시작되는 상태가 됩니다.
Legacy mode	ON/OFF, 기본값은 OFF 입니다. OFF: 표준 PD 장치만 지원되며 감지 저항은 19k~26.5k 이고 감지 커패시턴스는 150nF 미만입니다. ON: 비표준 PD 장치를 지원하고 감지 저항 및 정전 용량 값이 표준 값을 초과하는 일부 PD 장치에 전원을 공급할 수 있습니다.

표 3- 19 PoE 인터페이스 설정 메뉴

3.6 Security

3.6.1 Port Security

3.6.1.1 개요

포트 보안 기능은 포트의 유효한 MAC 주소 수를 제한하여 불법 사용자가 포트에 접근하는 것을 제한합니다. 불법 MAC 패킷은 직접 폐기됩니다. 적법한 MAC 은 정적으로 또는 동적으로 생성될 수 있습니다. 정적으로 허용할 MAC 은 사용자 설정을 통해 생성됩니다. 동적으로 허용할 MAC 은 MAC 주소 학습 기능을 통해 동적으로 생성됩니다.

포트의 보안 주소 개수가 설정된 최대 보안 주소 개수에 도달하면 새로운 MAC 접속 포트는 불법 MAC 으로 인식되어 위반 이벤트가 발생합니다. 사용자는 위반 이벤트가 발생할 때 수행할 작업을 각각 포트를 제한하거나 종료하도록 설정할 수 있습니다.

제한: 불법 MAC 데이터 전달을 금지하고 알람 로그 프롬프트 정보를 생성합니다. 불법 MAC 은 MAC 주소 에이징 시간 내에 해당 포트에 대한 접근을 금지합니다. 종료 및 종료 포트 없음을 통해 복원할 수 있습니다.

종료: 포트를 강제로 종료하며, 포트 복구 시간을 설정할 수 있습니다. 시간이 다 되면 포트가 자동으로 복구됩니다. 종료 명령 없이 종료를 통해 복구할 수도 있습니다.

동적 보안 사용자를 정적 보안 사용자로 변환하려면 포트에서 고정 기능을 활성화하면 됩니다. 포트에서 고정 기능이 활성화되면 포트에서 학습된 동적 사용자는 정적 사용자로 존재하게 됩니다. 설정이 저장되면 장치를 다시 시작한 후에도 장치가 계속 존재합니다.

NOTE:

- 일반 물리적 포트, LACP 포트와 같은 L2 포트 설정 포트 보안만 지원합니다.
- 액세스 모드에서는 포트 보안 설정만 지원합니다.
- LACP 포트는 지원하지 않습니다.
- SPAN 대상 포트는 지원하지 않습니다.
- 수동 MAC 주소로 설정된 포트에서는 포트 보안기능 설정을 지원하지 않습니다.

3.6.1.2 포트 보안 설정

1. Configuration > Security > Port security 메뉴에서 Port security 페이지로 접속합니다.

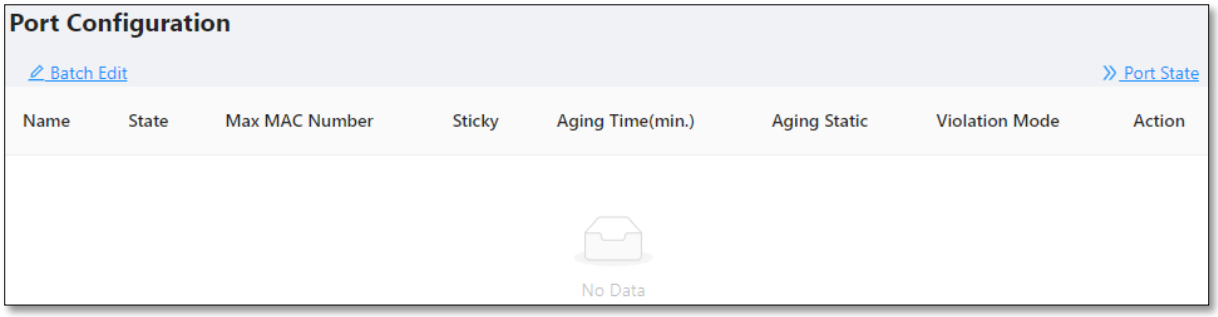


그림 3- 43 포트 보안 상태 페이지

2. Batch Edit 버튼을 클릭하여 "Port Configuration" 페이지로 접속합니다.

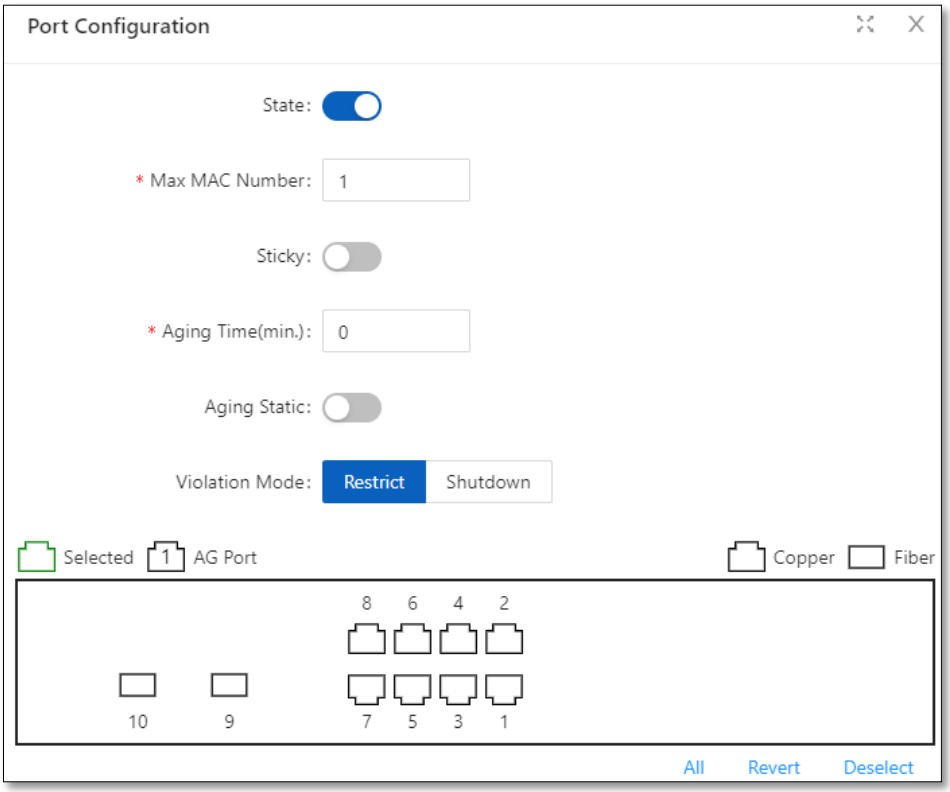


그림 3- 44 포트 보안 설정 페이지

메뉴		설명
Port Configuration	State	포트 보안을 활성화/비활성화합니다.
	Max MAC Number	포트에 대한 최대 보안 MAC 주소 수를 설정합니다. 기본 최대 보안 주소 수는 1 이고 범위는 다음과 같습니다.<1-1024>
	Sticky	Sticky 기능을 켜거나 끕니다.
	Aging Time(min)	보안 주소 만료 시간(분)을 설정합니다. 기본 에이징 시간은 0 이며, 이는 에이징 기능이 꺼진다는 의미입니다. 시간 범위<0-1440> 기본 에이징 기능은 동적 및 고정 보안 주소에만 적용됩니다.
	Aging Static	정적 보안 주소 에이징 기능을 활성화합니다.
	Violation Mode	포트 보안 위반 처리, 기본 위반 구성 모드는 제한입니다. 제한: 불법 사용자 데이터 전달을 금지하고 프롬프트를 기록합니다. 종료: 인터페이스를 종료하고 오류가 발생한 복구 시간이 지나면 통과를 재개합니다.

표 3- 20 포트 보안 설정 메뉴

3. Configuration > Security > MAC Configuration 메뉴에서 MAC Configuration 페이지로 접속합니다.

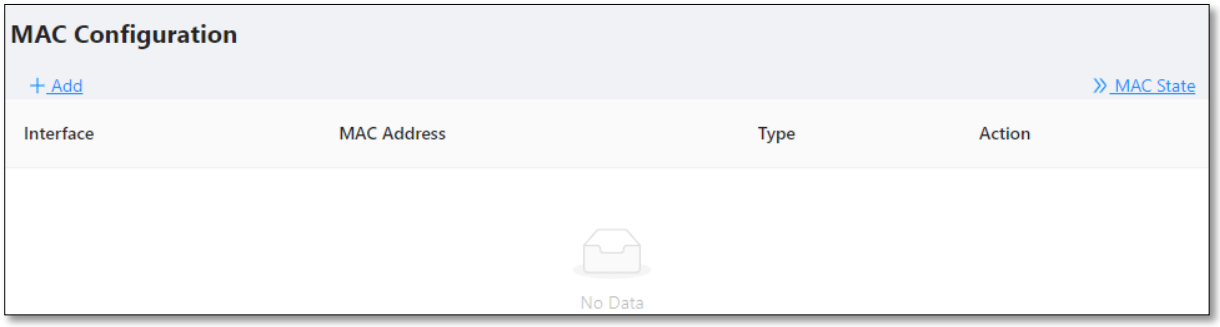


그림 3- 45 MAC 주소 설정 요약

다음과 같이 +ADD 를 클릭하여 MAC 설정 페이지로 들어갑니다

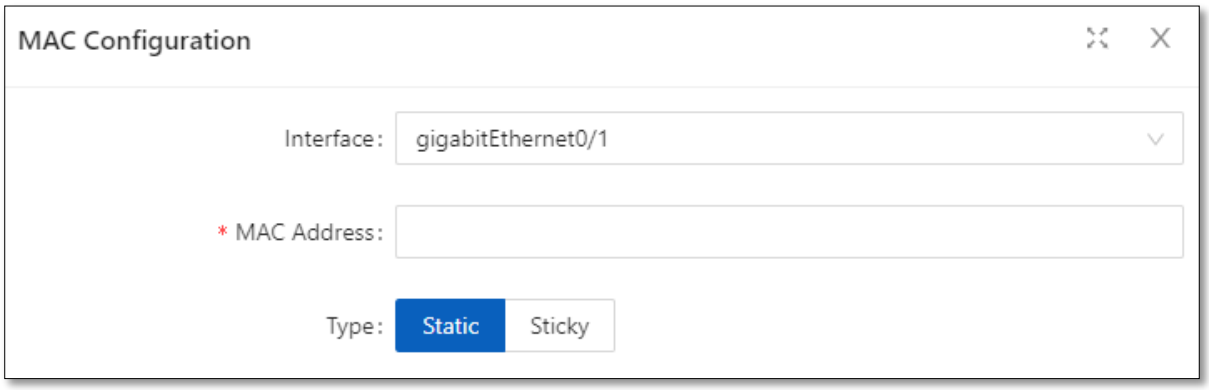


그림 3- 46 MAC 설정 페이지

메뉴		설명
MAC Configuration	Interface	설정할 인터페이스를 선택합니다.
	MAC Address	고정 보안 주소를 설정합니다. 보안 주소 형식은 XXXX.XXXX.XXXX 입니다. 보안 주소는 브로드캐스트 또는 멀티캐스트 주소로 설정할 수 없습니다.
	Type	MAC 주소를 동적 또는 고정으로 설정합니다.

표 3- 21 MAC 주소 설정 메뉴

3.6.2 IP Source Guard

3.6.2.1 개요

IP Source Guard

IP Source Guard 바인딩 기능은 IP+MAC 바인딩을 준수하는 IP 패킷이 해당 포트를 통과하도록 하고, 맞지 않는 패킷은 바로 폐기함으로써 IP/MAC 스푸핑 공격을 방지하는 목적을 달성합니다. IP Source Guard 의 바인딩 메뉴는 주로 IP dhcp 스누핑 환경의 사용자 정적 설정과 동적 획득이라는 두 가지 소스에서 나옵니다.

사용자 정적 설정: 주로 LAN 에서 IP 주소가 정적으로 설정된 호스트 사용자를 위한 것입니다.

IP dhcp 스누핑 동적 획득: 주로 근거리 통신망에서 dhcp 를 통해 IP 주소를 동적으로 획득하는 호스트 사용자에 응답합니다.

IP/MAC 스푸핑 공격: 불법 MAC 사용자는 액세스 ID 합법화를 실현하기 위해 합법적인 소스 IP 가 포함된 IP 패킷을 보냅니다.

ARP Check

Arp-check(ARP 패킷 검사) 기능은 해당 포트 아래의 모든 ARP 패킷을 필터링하고 불법적인 ARP 패킷을 모두 폐기하므로 네트워크에서의 ARP 스푸핑을 효과적으로 방지하고 네트워크의 안정성을 향상시킬 수 있습니다. Arp-check 기능을 지원하는 장치에서 Arp-check 기능은 IP Source Guard 와 같은 보안 응용 모듈에서 생성된 합법적인 사용자 정보(IP+MAC)를 기반으로 해당 ARP 필터링 정보를 생성하여 다음을 실현할 수 있습니다. 네트워크에서 불법 ARP 패킷 필터링 합니다.

3.6.2.2 IP Source Guard 설정

1. Configuration > Security > IP Source Guard 메뉴에서 IP Source Guard 페이지에 접속합니다.

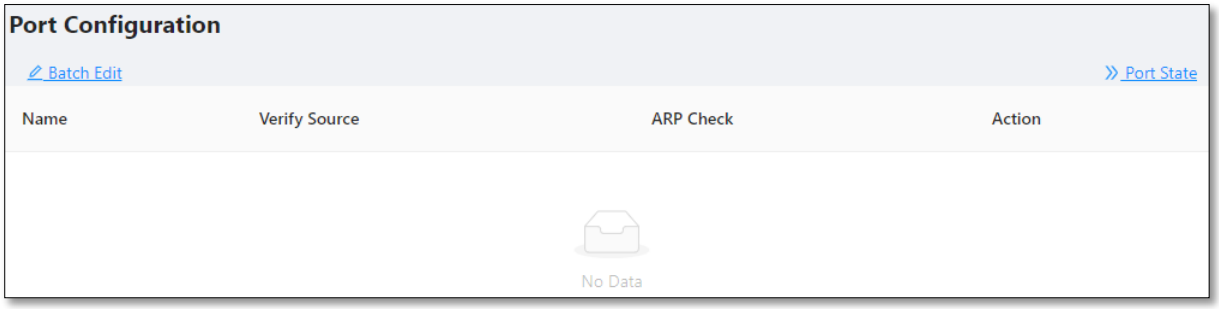


그림 3- 47 IP Source Guard 페이지

2. Batch Edit 을 클릭하고 "Port Configuration" 페이지에 접속합니다.

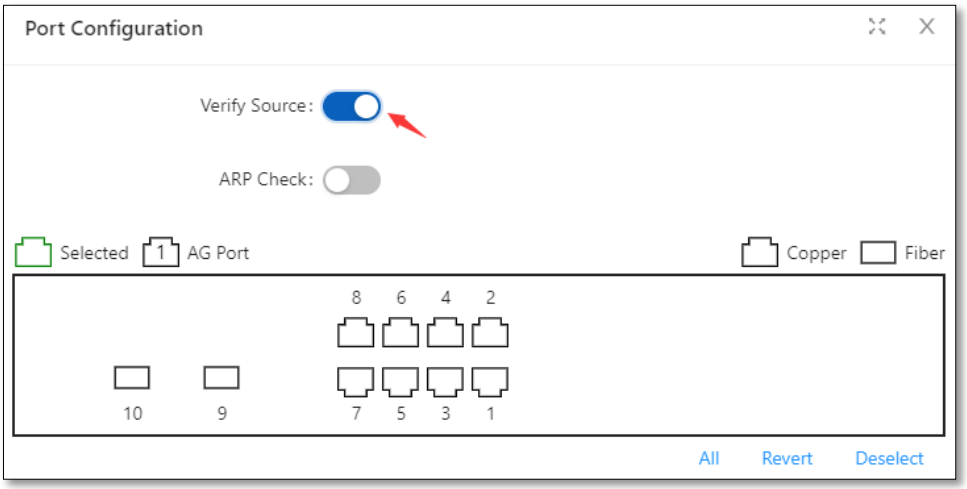


그림 3- 48 IP Source Guard 포트 설정

Apply 버튼을 클릭하면 생성된 규칙이 다음과 같이 요약 페이지에 표시됩니다.

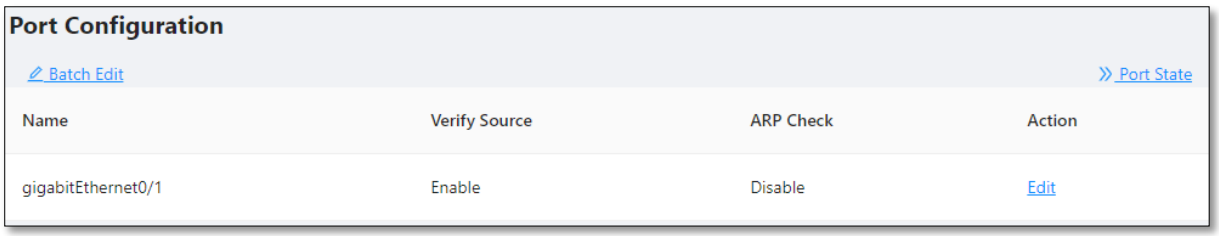


그림 3- 49 포트 설정

3. +ADD 버튼을 클릭하여 "User Configuration" 페이지로 접속합니다. 아래의 그림처럼 인터페이스 메뉴에서 포트, VID , IP 주소, MAC 주소등을 선택합니다.

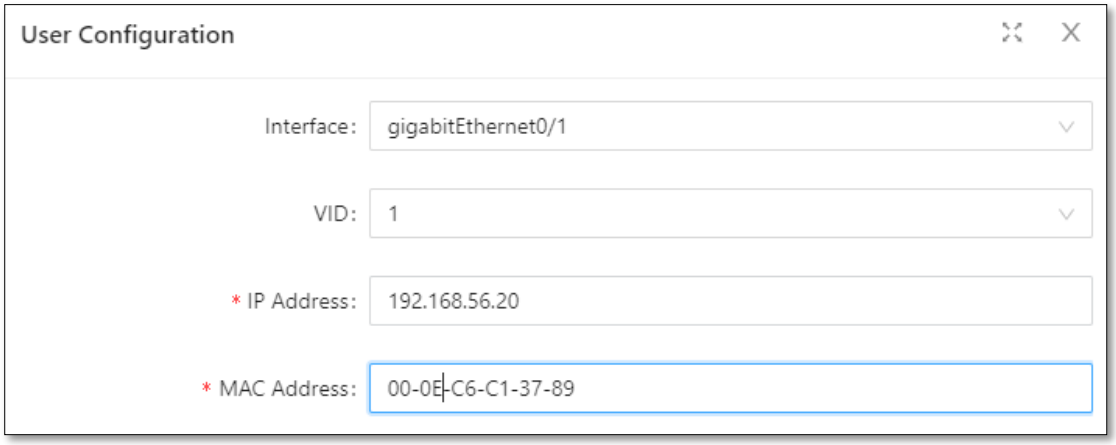


그림 3- 50 사용자 설정

4. Apply 버튼을 클릭하면 생성된 규칙이 다음과 같이 요약 페이지에 표시됩니다.

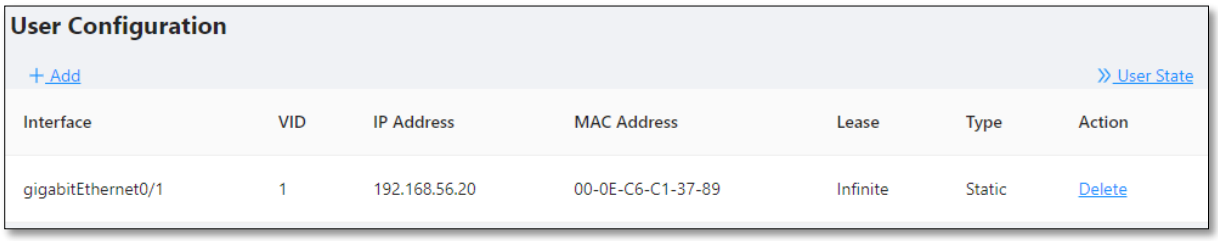


그림 3- 51 IP Source Guard 규칙 요약

3.6.2.3 ARP Check 설정

1. Configuration > Security > IP Source 메뉴에서 IP Source Guard Summary 페이지로 접속합니다.
2. Batch Edit 버튼을 클릭하고 포트 패널메뉴에서 설정할 인터페이스를 선택한 다음 클릭합니다.

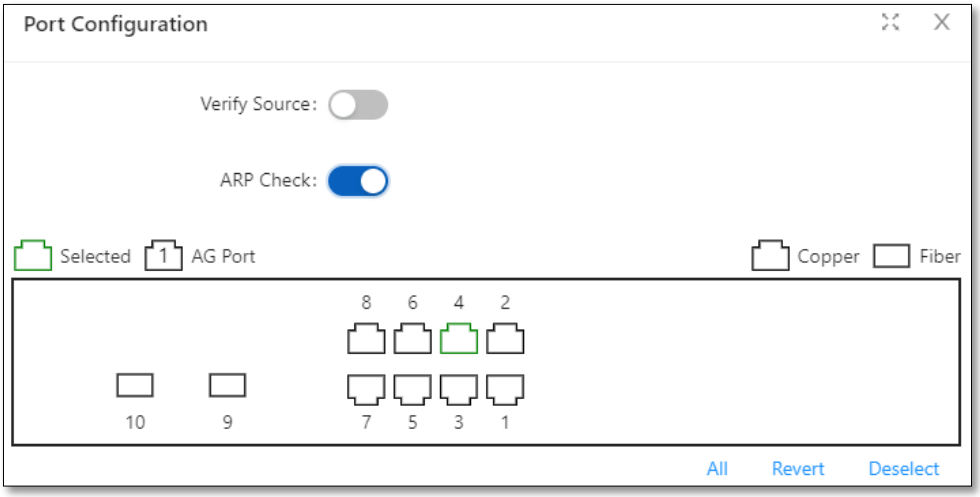


그림 3- 52 IP Source Guard ARP Check

3. +ADD 버튼을 클릭하여 "User Configuration" 페이지로 접속합니다.

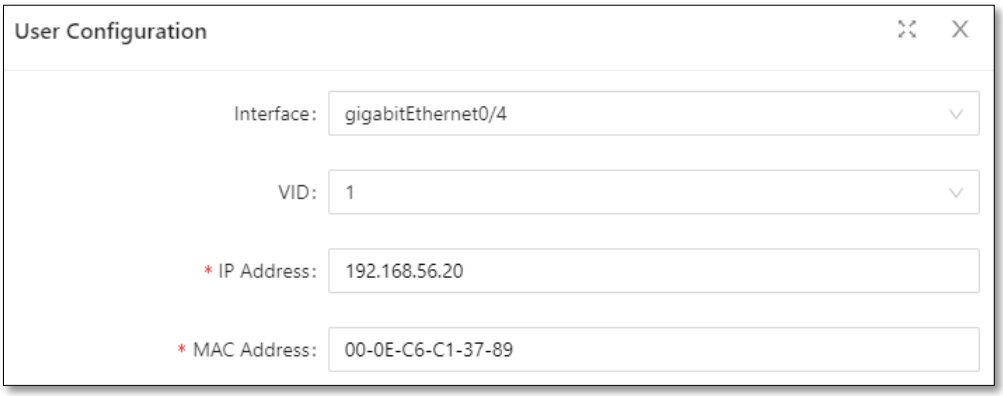


그림 3- 53 IP Source Guard 사용자 설정

4. Apply 버튼을 클릭하면 생성된 규칙이 다음과 같이 요약 페이지에 표시됩니다.

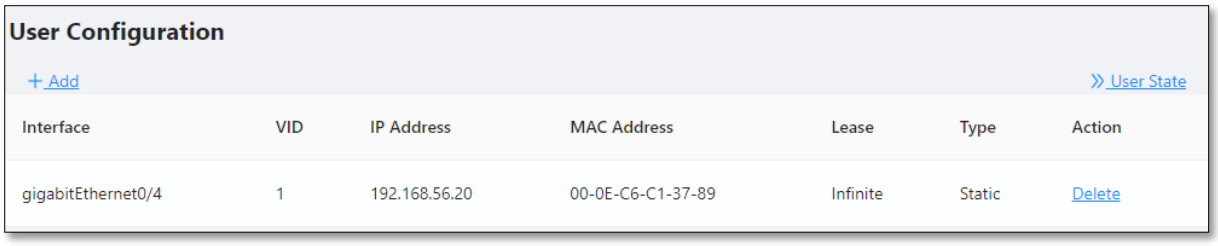


그림 3- 54 ARP Check 규칙

3.6.3 Dot1X

3.6.3.1 개요

802.1X(Dot1X) 프로토콜은 무선 LAN(WLAN) 보안을 위한 IEEE 802 LAN/WAN 위원회에서 제안되었습니다. 이는 이더넷에서 공통 포트 액세스 제어 메커니즘으로 널리 사용되었습니다. 포트 기반 액세스 제어 프로토콜인 802.1X 는 포트 수준에서 액세스 장치를 인증하고 제어합니다. 액세스 제어 장치의 802.1X 지원 포트에 연결된 장치는 인증을 통과한 후에만 LAN 의 리소스에 액세스할 수 있습니다.

- 802.1X 의 아키텍처

802.1X 는 일반적인 클라이언트/서버 모델에서 동작하며 아래와 같이 클라이언트, 장치 및 서버의 세 가지 메뉴를 지원합니다.

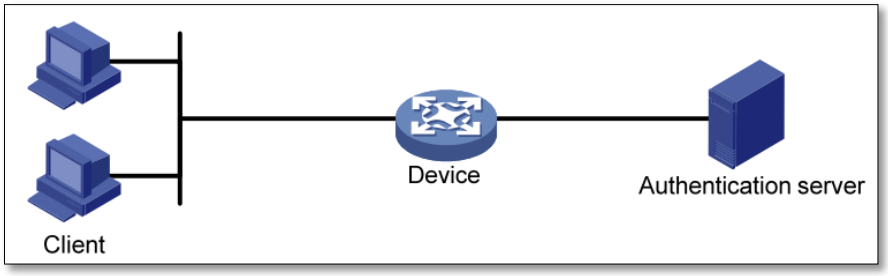


그림 3- 55 802.1x

- 클라이언트는 LAN 에 대한 액세스를 원하는 개체입니다. LAN 세그먼트의 한쪽 끝에 상주하며 LAN 세그먼트의 다른 쪽 끝에 있는 장치에 의해 인증됩니다. 클라이언트는 일반적으로 PC 와 같은 사용자 측 장치입니다. 802.1X 인증은 802.1X 지원 클라이언트 프로그램이 클라이언트에서 시작될 때 트리거 됩니다. 클라이언트 프로그램은 EAPOL(Extensible Authentication Protocol over LAN)을 지원해야 합니다.
- LAN 세그먼트의 다른 쪽 끝에 있는 장치는 연결된 클라이언트를 인증합니다. 장치는 일반적으로 802.1X 지원 네트워크 장치이며 클라이언트가 LAN 에 액세스할 수 있도록 액세스 포트(물리적 또는 논리적)를 제공합니다.
- 서버는 장치에 인증 서비스를 제공하는 개체입니다. 일반적으로 RADIUS(Remote Authentication Dial-in User Service)를 실행하는 서버는 사용자에 대한 인증, 권한 부여 및 계정 서비스를 수행하는 역할을 합니다.

- 802.1X 의 인증 모드

802.1X 인증 시스템은 EAP(확장 가능 인증 프로토콜)를 사용하여 클라이언트, 장치 및 인증 서버 간에 인증 정보를 교환합니다.

- 클라이언트와 장치 사이에서 EAP 프로토콜 패킷은 EAPOL 을 사용하여 캡슐 화되어 LAN 에서 전송됩니다.
- 장치와 RADIUS 서버 간에 EAP 프로토콜 패킷은 EAP 릴레이 및 EAP 종료의 두 가지 모드로 교환될 수 있습니다. EAP 릴레이 모드에서 EAP 패킷은 장치의 EAP over RADIUS(EAPOR) 패킷에 캡슐화 된 다음 장치에서 RADIUS 서버로 릴레이 됩니다. EAP 종료 모드에서는 EAP 패킷이 장치에서 종료되고 PAP(암호 인증 프로토콜) 또는 CHAP(Challenge Handshake 인증 프로토콜) 특성을 사용하여 RADIUS 패킷으로 변환된 다음 RADIUS 서버로 전송됩니다.

- 802.1X 의 기본 개념

802.1X 에는 제어된 포트/비제어 포트, 승인된 상태/비 승인 상태 및 제어 방향이라는 기본 개념이 포함되어 있습니다.

- 제어되는 포트와 비제어 포트

장치는 클라이언트가 LAN 에 액세스할 수 있는 포트를 제공합니다. 각 포트는 제어된 포트와 제어되지 않은 포트라는 두 개의 논리적 포트가 하나로 통합된 것으로 간주될 수 있습니다. 포트에 도착하는 모든 패킷은 두 논리 포트 모두에서 볼 수 있습니다.

- 제어되지 않은 포트는 인 바운드 및 아웃 바운드 방향 모두에서 항상 열려 EAPOL 프로토콜 패킷이 통과할 수 있도록 하여 클라이언트가 항상 인증 패킷을 보내고 받을 수 있도록 보장합니다.
- 제어되는 포트는 승인된 상태일 때만 데이터 트래픽이 통과할 수 있도록 열려 있습니다.

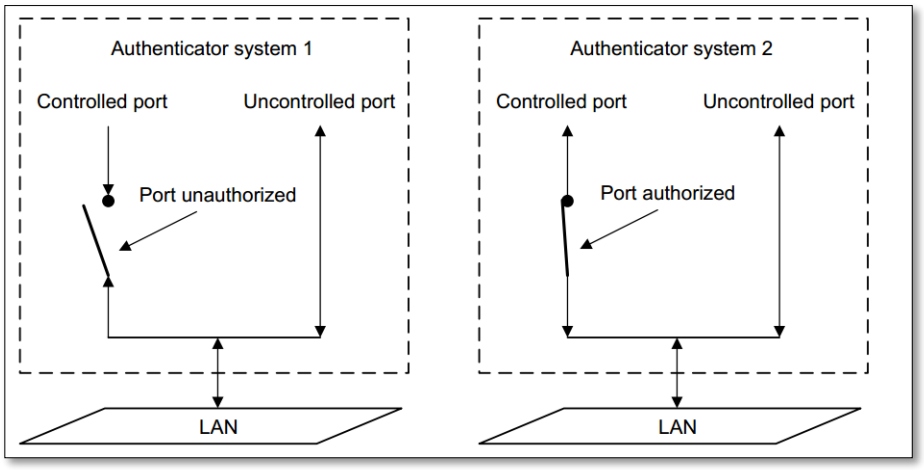


그림 3- 56 제어되는 포트의 승인 및 비 승인 상태

제어된 포트는 다음과 같이 인증 결과에 따라 승인된 상태 또는 승인되지 않은 상태일 수 있습니다.

포트 인증 모드를 다음 중 하나로 설정하여 포트의 포트 인증 상태를 제어할 수 있습니다.

- Force-Authorized : 포트를 인증 상태로 설정하여 포트 사용자가 인증 없이 네트워크에 액세스할 수 있도록 합니다.
- Force-Unauthorized: 포트를 승인되지 않은 상태로 전환하여 포트 사용자의 모든 액세스 요청을 거부합니다.
- Auto: 처음에는 포트를 인증되지 않은 상태로 설정하여 EAPOL 패킷만 통과하도록 허용하고, 사용자가 인증을 통과한 후에는 네트워크에 대한 액세스를 허용하도록 포트를 인증된 상태로 전환합니다. 이것이 가장 일반적인 선택입니다.

• Control dirction

802.1X 인증은 클라이언트나 장치에서 시작할 수 있습니다.

• 802.1X authentication triggering

클라이언트는 장치에 EAPOL-Start 패킷을 전송하여 원치 않는 인증을 시작할 수 있습니다. 패킷의 대상 주소는 IEEE 802.1X 프로토콜에 의해 지정된 멀티캐스트 주소인 01-80-C2-00-00-03 입니다. 네트워크의 일부 장치는 위의 대상 주소로 멀티캐스트 패킷을 지원하지 않을 수 있으며 결과적으로 클라이언트의 인증 요청을 수신하지 못할 수 있습니다. 이 문제를 해결하기 위해 장치는 브로드캐스트 MAC 주소를 대상 주소로 사용하는 EAPOL-Start 패킷도 지원합니다.

- 장치의 원치 않는 트리거링

장치는 인증되지 않은 클라이언트에 EAP 요청/ID 패킷을 정기적으로(기본적으로 30 초마다) 전송하여 인증을 트리거 할 수 있습니다. 이 방법은 인증을 트리거 하기 위해 원치 않게 EAPOL-Start 패킷을 보낼 수 없는 클라이언트(예: Windows XP 에서 제공되는 802.1X 클라이언트 응용 프로그램을 실행하는 클라이언트)를 인증하는 데 사용할 수 있습니다.

- 802.1X 의 인증 프로세스

802.1X 장치는 EAP 릴레이와 EAP 종료라는 두 가지 모드로 원격 RADIUS 서버와 통신합니다. 다음은 예제에서 클라이언트에 의해 트리거 되는 두 가지 모드의 802.1X 인증 절차를 설명합니다.

- EAP 릴레이

EAP 릴레이는 IEEE 802.1X 에 정의되어 있습니다. 이 모드에서는 EAP 패킷이 RADIUS 와 같은 상위 계층 프로토콜을 통해 전달되므로 복잡한 네트워크를 통과하여 인증 서버에 도달할 수 있습니다. 일반적으로 EAP 를 중계하려면 RADIUS 서버가 EAP 패킷을 캡슐화하고 EAP Message 속성을 전달하는 RADIUS 패킷을 보호하는 데 사용되는 EAP-Message 및 Message-Authenticator 의 EAP 속성을 지원해야 합니다.

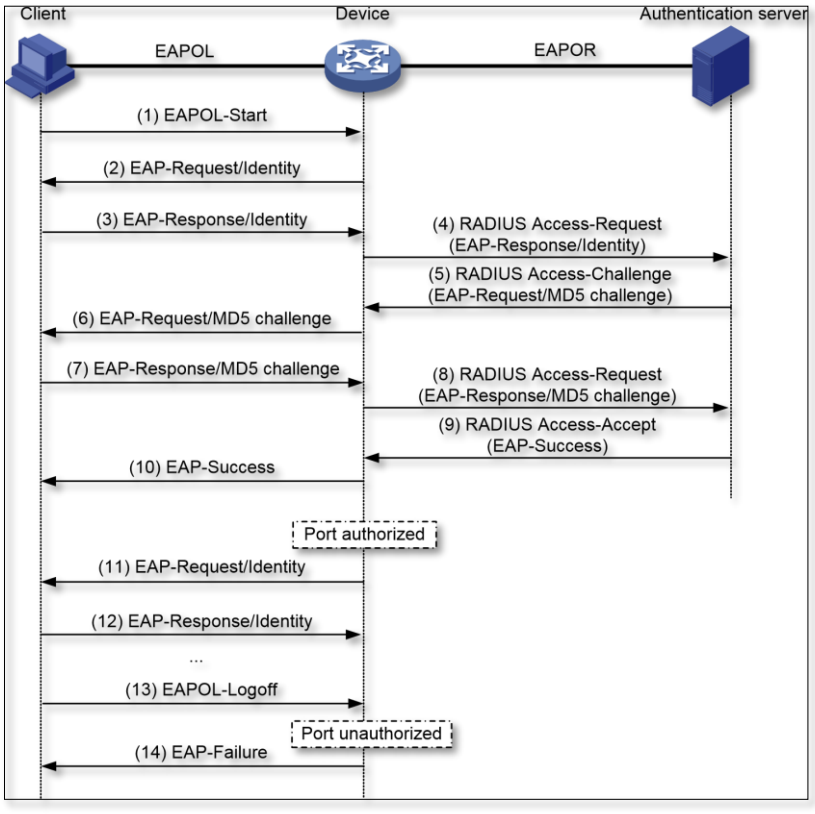


그림 3- 57 EAP-MD5 와의 메시지 교환 절차

1. 사용자가 802.1X 클라이언트 소프트웨어를 실행하고 등록된 사용자 이름과 비밀번호를 입력하면 802.1X 클라이언트 소프트웨어는 EAPOL-Start 프레임을 생성하고 이를 장치로 전송하여 인증 프로세스를 시작합니다.
2. EAPOL-Start 프레임을 수신하면 장치는 클라이언트의 사용자 이름에 대한 EAPRequest/Identity 패킷으로 응답합니다.
3. 클라이언트가 EAP-요청/ID 패킷을 수신하면 EAP-응답/ID 패킷에 사용자 이름을 캡슐화 하여 해당 패킷을 클라이언트로 보냅니다. 장치.
4. EAP 응답/ID 패킷을 수신하면 장치는 RADIUS 액세스 요청 패킷에 포함된 패킷을 인증 서버에 전달합니다.
5. RADIUS 액세스 요청 패킷을 수신하면 RADIUS 서버는 식별 정보를 사용자 정보 테이블과 비교하여 해당 비밀번호 정보를 얻습니다. 그런 다음 무작위로 생성된 챌린지를 사용하여 비밀번호 정보를 암호화하고 RADIUS Access-Challenge 패킷을 통해 챌린지 정보를 장치로 보냅니다.
6. RADIUS 액세스-챌린지 패킷을 수신한 후 장치는 포함된 EAP-요청/MD5 챌린지 패킷을 클라이언트에 중계합니다.
7. EAP-요청/MD5 챌린지 패킷을 수신하면 클라이언트는 제공된 챌린지를 사용하여 비밀번호 부분을 암호화하고(이 프로세스는 되돌릴 수 없음) EAP-응답/MD5 챌린지 패킷을 생성한 다음 해당 패킷을 장치로 보냅니다.
8. EAP-Response/MD5 Challenge 패킷을 수신한 후 장치는 RADIUS Access-Request 패킷을 통해 해당 패킷을 인증 서버로 중계합니다.
9. RADIUS Access-Request 패킷을 수신하면 RADIUS 서버는 자체적으로 생성된 비밀번호 정보와 함께 패킷에 캡슐화 된 비밀번호 정보입니다. 두 개가 동일하면 인증 서버는 사용자가 유효한 것으로 간주하고 장치에 RADIUS 액세스 허용 패킷을 보냅니다.
10. RADIUS Access-Accept 패킷을 수신하면 장치는 포트를 열어 클라이언트의 액세스 요청을 승인합니다. 클라이언트가 온라인 상태가 되면 장치는 주기적으로 클라이언트에 핸드 셰이크 요청을 보내 클라이언트가 아직 온라인 상태인지 확인합니다. 기본적으로 두 번의 연속 핸드 셰이크 시도가 실패하면 장치는 클라이언트가 오프라인이 되었다고 결론을 내리고 필요한 작업을 수행하여 클라이언트가 오프라인이 되는 시기를 장치가 항상 알 수 있도록 보장합니다.

11. 또한 클라이언트는 EAPOL-로그오프 프레임을 장치에 보내 원치 않게 오프라인 상태로 전환할 수도 있습니다. 이 경우 장치는 포트 상태를 Authorized 에서 Unauthorized 로 변경하고 EAP-Failure 패킷을 클라이언트로 보냅니다.

3.6.3.2 Dot1X 설정

1. Security > Dot1x> 메뉴에서 802.1X Global Configuration , Port Configuration 페이지로 접속합니다.

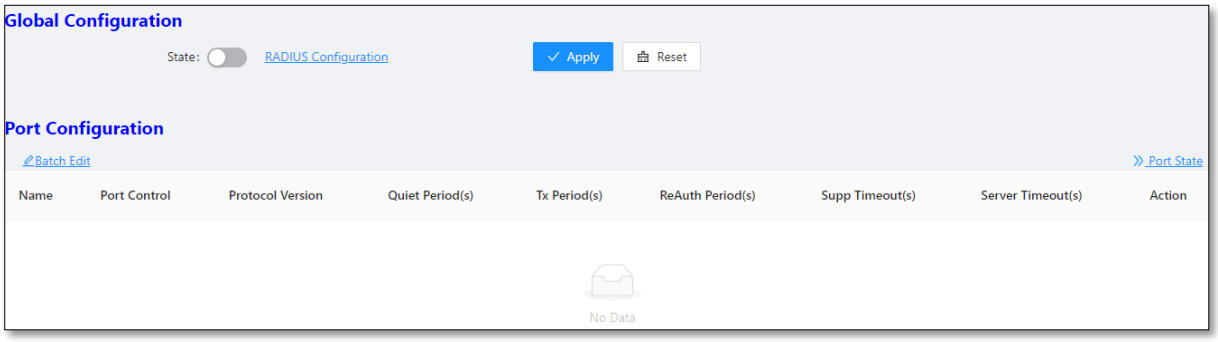


그림 3- 58 802.1X 설정

메뉴		설명
Global Configuration	State	스위치에서 802.1X 기능을 활성화합니다.
	RADIUS Configuration	RADIUS 설정 인터페이스로 이동하려면 클릭하세요.

표 3- 22 802.1X 설정 메뉴

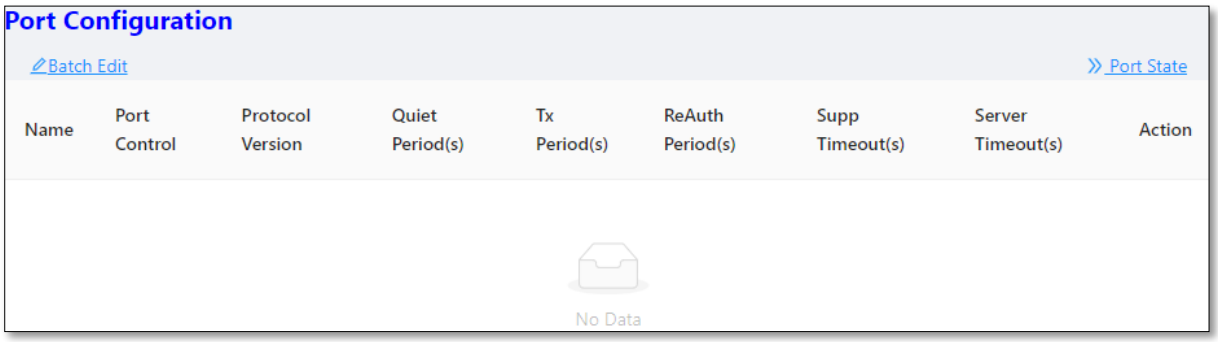


그림 3- 59 802.1X 포트 설정

메뉴		설명
Port Configuration	Name	물리적 인터페이스 이름
	Port Control	포트 제어 모드

	Protocol Version	Eapol 프로토콜 버전, 기본 버전 2
	Quiet Period(s)	클라이언트와의 인증 교환 실패 후 스위치가 Quiet Period 에 남아 있는 시간(초)을 설정합니다. 범위는 0~65,535 초입니다. 기본값은 60 입니다. 스위치가 클라이언트를 인증할 수 없으면 스위치는 일정 기간 동안 유휴 상태를 유지한 후 다시 시도합니다. 유휴 시간은 정적 기간 값에 따라 결정됩니다.
	Tx Period(s)	요청을 재전송하기 전에 스위치가 클라이언트의 EAP 요청/ID 프레임에 대한 응답을 기다리는 시간(초)을 설정합니다. 범위는 1~65,535 초입니다. 기본값은 30 입니다.
	ReAuth Enabled	클라이언트의 주기적인 재인증을 활성화합니다.
	ReAuth Period(s)	재인증 시도 간격(초)을 지정하거나 스위치가 RADIUS 제공 세션 시간 초과를 사용하도록 합니다. 범위는 1~65,535 입니다. 기본값은 3600 초입니다. 이 명령은 정기적 재인증이 활성화된 경우에만 스위치 동작에 영향을 미칩니다.
	Supp Timeout(s)	요청을 재전송하기 전에 스위치가 클라이언트로부터 EAP-요청/MD5 챌린지 프레임에 대한 응답을 기다리는 시간(초)을 설정합니다. 범위는 1~65,535 초입니다. 기본값은 30 입니다.
	Server Timeout(s)	스위치가 서버의 RADIUS 액세스 요청 패킷에 대한 응답을 기다리는 시간(초)을 설정합니다. 범위는 1~65,535 초입니다. 기본값은 30 입니다.

표 3- 23 802.1X 포트 설정 메뉴

3.6.4 MAC Auth

3.6.4.1 개요

MAC 주소 인증은 모든 유효한 사용자의 데이터베이스가 포함된 RADIUS 서버를 사용하여 지원됩니다. 인터페이스에서 mac-auth 옵션이 활성화되면 수신 프레임의 모든 소스 MAC 주소가 인증을 위해 전송됩니다. RADIUS 서버에 소스 주소의 사용자 이름과 비밀번호가 설정되어 있으면 인증이 성공하고, 그렇지 않으면 실패합니다. 인증이 성공하면 원본 MAC 가 전달이 활성화된 전달 테이블에 추가됩니다. 오류가 발생하는 경우 소스 MAC 은 폐기된 상태로 전달 테이블에 추가되거나 제한된 VLAN 에 추가됩니다.

NOTE:

- 설정된정적 MAC 이 자동 MAC 과 동일한 경우 MAC 주소 인증 실패 후 MAC 자동 기능은 유효하지 않습니다.

3.6.4.2 MAC 인증 설정

- MAC 인증 요약 표시

1. Configuration > Security > MAC Authentication 메뉴에서 MAC Authentication 페이지에 접속합니다.

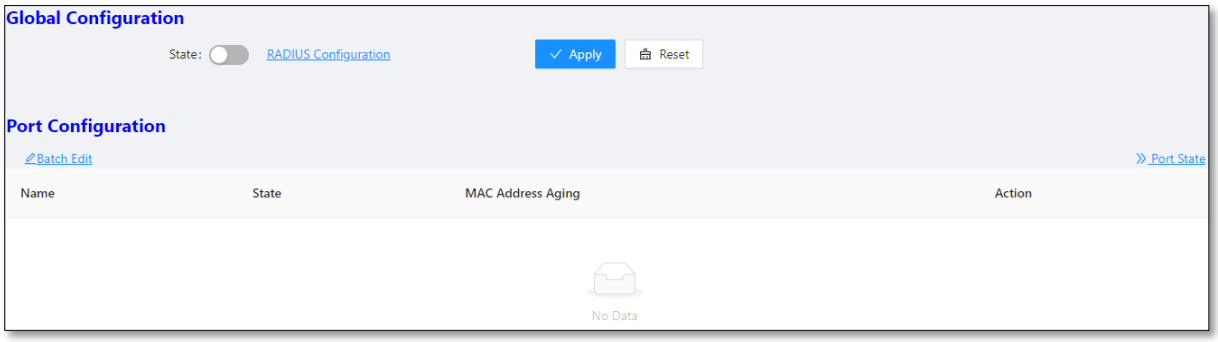


그림 3- 60 MAC 인증 요약 페이지

메뉴		설명
Global Configuration	State	스위치에서 802.1X 기능을 활성화합니다.
	RADIUS Configuration	RADIUS 설정 인터페이스로 이동하려면 클릭하세요.
Port Configuration	Name	물리적 인터페이스 이름
	State	MAC 인증 상태 표시
	MAC Address Aging	상태를 표시하다 MAC 주소 에이징
	Action	규칙을 편집하려면 클릭하세요.

표 3- 24 MAC 인증 요약 메뉴

- MAC 인증 설정

1. MAC 인증 활성화 Configuration > Security > MAC Authentication 메뉴에 접속합니다. "Global Configuration" 에서 Apply 버튼을 클릭하면 MAC Auth 기능이 활성화됩니다.
2. Batch Edit 클릭하여 "Port Configuration" 메뉴로 접속합니다.

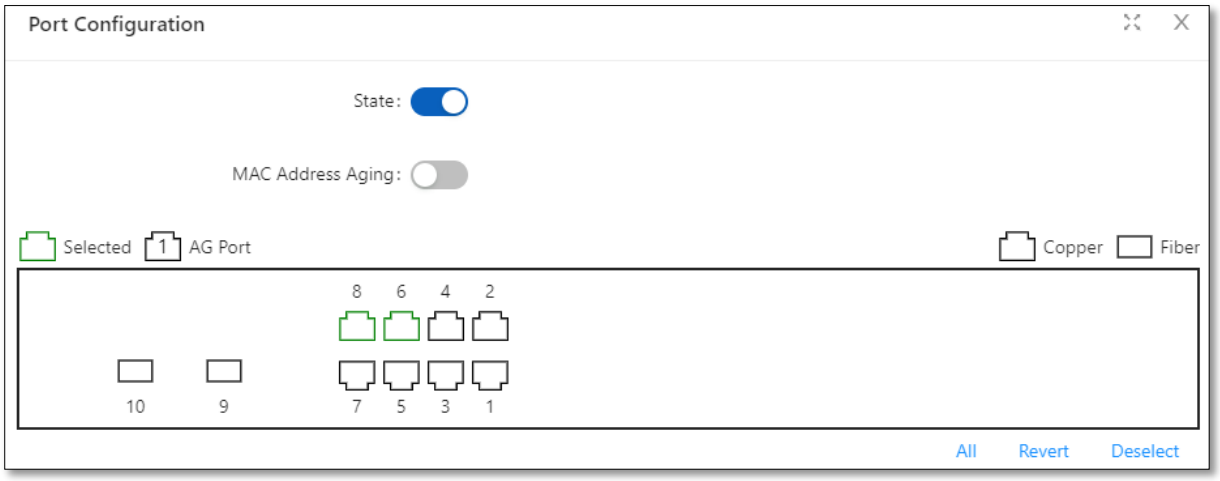


그림 3- 61 MAC 인증 포트 설정

3.6.5 RADIUS

3.6.5.1 개요

RADIUS(Remote Authentication Dial-In User Service)는 AAA(인증, 권한 부여 및 계정 관리)를 구현하기 위한 프로토콜입니다. RADIUS 는 클라이언트/서버 모델을 사용하는 분산 정보 상호 작용 프로토콜입니다. RADIUS 는 무단 액세스로부터 네트워크를 보호할 수 있으며 높은 보안과 원격 사용자 액세스가 모두 필요한 네트워크 환경에서 자주 사용됩니다. RADIUS 는 UDP 를 사용하며 패킷 형식과 메시지 전송 메커니즘은 UDP 를 기반으로 합니다. 인증에는 UDP 포트 1812 를 사용하고 계정에는 1813 을 사용합니다. 액세스 방법이 다양해짐에 따라 RADIUS 는 이더넷 액세스, ADSL 액세스 등 더 많은 액세스 방법을 지원하도록 확장되었습니다. 접속 서비스 제공 시 인증 및 권한 부여를 사용하고, 계정을 사용하여 네트워크 자원의 사용 정보를 수집하고 기록합니다.

- 클라이언트 / 서버 모델
  - 클라이언트: RADIUS 클라이언트는 네트워크 전체에 위치한 NAS 에서 실행됩니다. 사용자 정보를 지정된 RADIUS 서버에 전달하고 응답에 따라 조치를 취합니다(예: 사용자 액세스 요청 거부 또는 수락).
  - 서버: RADIUS 서버는 네트워크 센터의 컴퓨터나 워크스테이션에서 실행되며 사용자 인증 및 네트워크 서비스 접속과 관련된 정보를 유지합니다. 연결 요청을 수신하고, 사용자를 인증하고, 처리 결과(예: 사용자 액세스 요청 거부 또는 수락)를 클라이언트에 반환합니다.

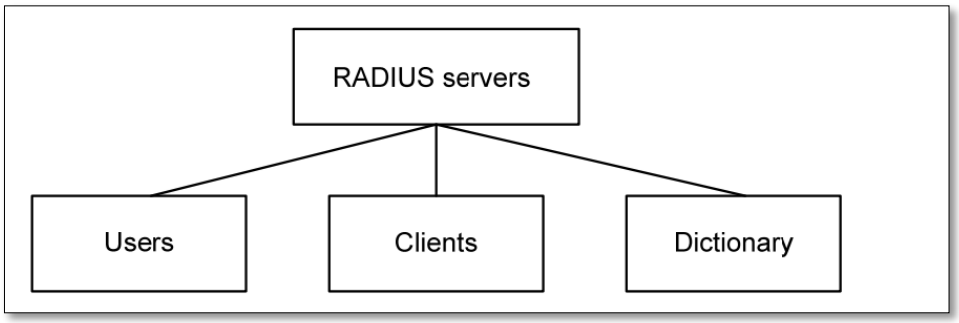


그림 3- 62 RADIUS 서버 설정 요소

- Users: 사용자 이름, 비밀번호, 적용된 프로토콜, IP 주소 등의 사용자 정보를 저장합니다.
- Client: 공유 키, IP 주소 등 RADIUS 클라이언트에 대한 정보를 저장합니다.

- Dictionary: RADIUS 프로토콜 속성의 의미와 해당 값에 대한 정보를 저장합니다.

• 보안 및 인증 메커니즘

RADIUS 클라이언트와 RADIUS 서버 간에 교환되는 정보는 네트워크를 통해 전송되지 않는 공유 키로 인증됩니다. 이는 정보 교환 보안을 강화합니다. 또한 안전하지 않은 네트워크에서 사용자 비밀번호를 가로채는 것을 방지하기 위해 RADIUS 는 비밀번호를 전송하기 전에 암호화합니다. RADIUS 서버는 PAP(Password Authentication Protocol) 및 PPP(Point-to-Point Protocol)의 CHAP(Challenge Handshake 인증 프로토콜)과 같은 여러 사용자 인증 방법을 지원합니다. 또한 RADIUS 서버는 다른 AAA 서버의 클라이언트 역할을 하여 인증 프록시 서비스를 제공할 수 있습니다.

• RADIUS 기본 메시지 교환 과정

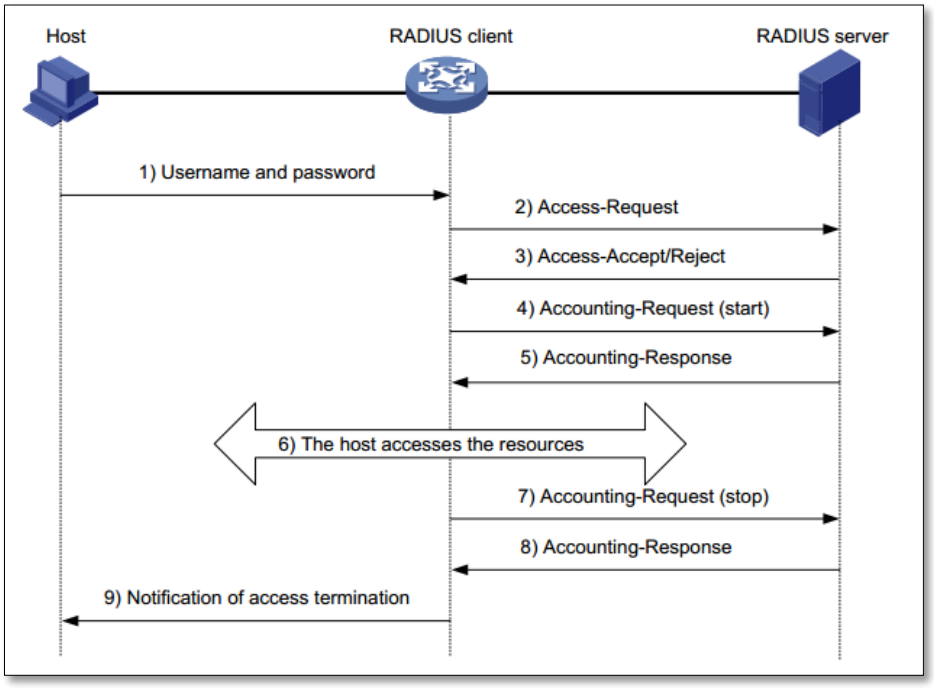


그림 3- 63 RADIUS 의 기본 메시지 교환 과정

1. 호스트는 RADIUS 클라이언트에 사용자 이름과 비밀번호를 전달하는 연결 요청을 시작합니다.
2. 사용자 이름과 비밀번호를 받은 RADIUS 클라이언트는 MD5(Message-Digest 5) 알고리즘과 공유 키를 사용하여 암호화된 사용자 비밀번호와 함께 RADIUS 서버에 인증 요청(액세스 요청)을 보냅니다.
3. RADIUS 서버는 사용자 이름과 비밀번호를 인증합니다. 인증이 성공하면 사용자의 인증 정보가 포함된 Access-Accept 메시지를 다시 보냅니다. 인증에 실패하면 액세스 거부 메시지가 반환됩니다.

4. RADIUS 클라이언트는 반환된 인증 결과에 따라 사용자를 허용하거나 거부합니다. 사용자를 허용하면 RADIUS 서버에 계정 시작 요청(Accounting-Request)을 보냅니다.
5. RADIUS 서버는 계정 시작 응답(Accounting-Response)을 반환하고 계정을 시작합니다.
6. 사용자가 네트워크 리소스에 액세스합니다.
7. 호스트는 RADIUS 클라이언트에게 연결을 끊도록 요청하고 RADIUS 클라이언트는 RADIUS 서버에 계정 중지 요청(Accounting-Request)을 보냅니다.
8. RADIUS 서버는 계정 중지 응답(Accounting-Response)을 반환하고 사용자 계정을 중지합니다.
9. 사용자가 네트워크 리소스에 대한 액세스를 중지합니다.

NOTE:

- RADIUS 계정 기능은 지원하지 않습니다.

3.6.5.2 RADIUS 설정

1. Configuration > Security > RADIUS 메뉴에서 RADIUS Global Configuration 페이지로 접속합니다.

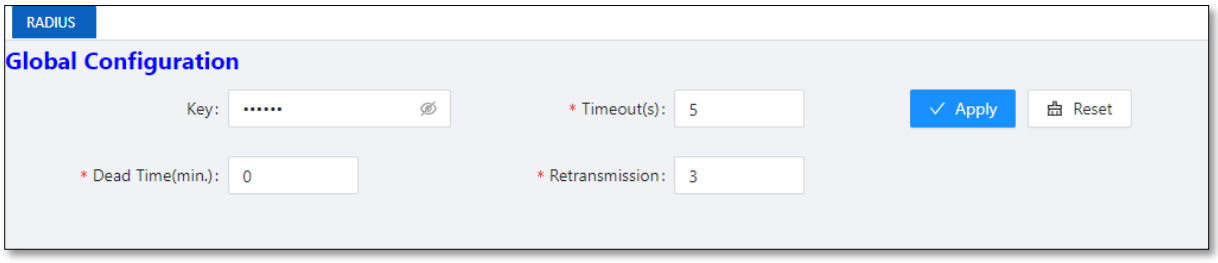


그림 3- 64 RADIUS 설정

메뉴		설명
Global Configuration	Key	기본 비밀번호 설정. 설정 가능, 읽을 수 없음; 선택적 설정
	Timeout	글로벌 서버 시간 초과. 선택적 설정
	Retransmission	글로벌 서버 재전송 선택적 설정
	Dead Time	서버 종료 기간; 선택적 설정; 기본값은 0 으로, 서버 종료 후 즉시 가동을 나타냅니다.

표 3- 25 RADIUS Grobal 설정

2. +Add 버튼을 클릭하여 RADIUS Server Configuration 페이지로 접속합니다.

메뉴	설명
IP	서버 IP 주소
Auth Port	서버 인증 포트 번호. 기본 1812
Key	서버 키; 설정되지 않은 경우 글로벌 설정
Timeout	서버 시간 초과; 기본 5 초
Retransmission	서버 재전송 횟수, 기본값은 3 회

표 3- 26 RADIUS Server 설정

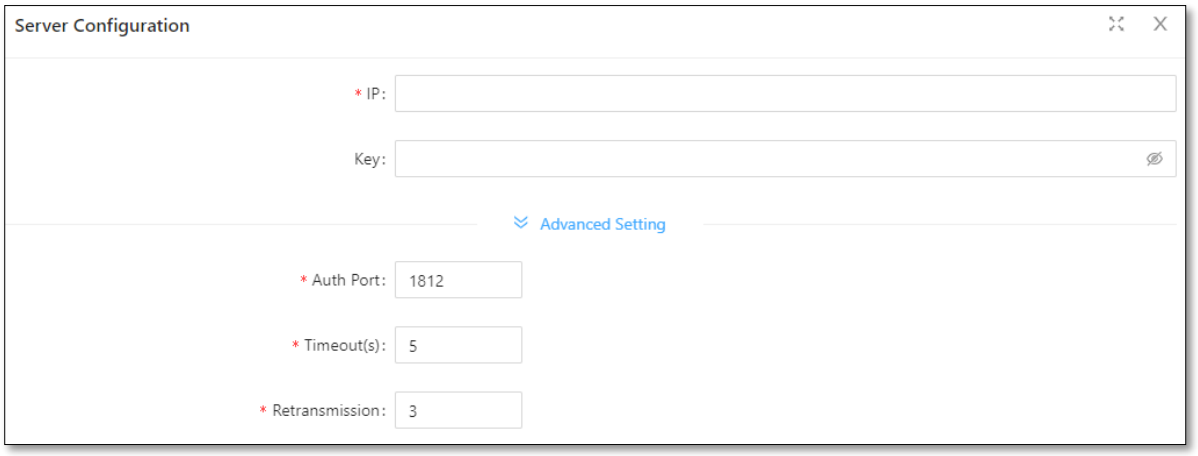


그림 3- 65 RADIUS Server 설정

3.7 Control

3.7.1 시리얼 서버

3.7.1.1 개요

시리얼 장치 서버는 직렬 장치를 이더넷에 연결하는 데 사용됩니다. 시리얼 장치 서버는 네트워크 데이터와 직렬 데이터의 양방향 변환 및 전송을 지원합니다. 시리얼 장치 서버는 다음과 같이 tcp-client 모드에서 동작합니다.

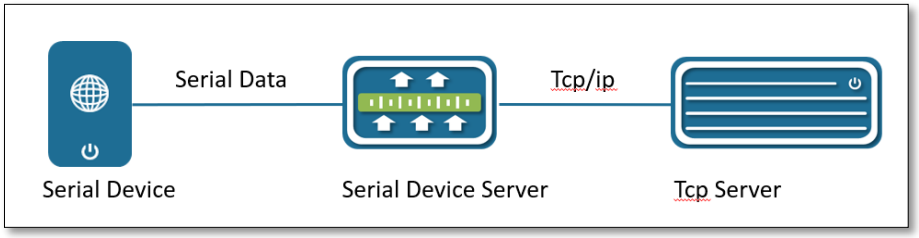


그림 3- 66 tcp-client 모드에서 시리얼 서버 동작

tcp-client 모드의 직렬 장치 서버는 TCP 네트워크 서버에 대한 클라이언트 연결을 제공합니다. 직렬 장치와 TCP 서버 간의 상호 작용을 실현하기 위해 적극적으로 연결을 시작하고 서버에 연결합니다. Tcp/Ip 및 직렬 데이터는 양방향으로 투명하게 전송됩니다. 직렬 장치 서버는 여러 TCP 클라이언트를 설정하여 다른 Tcp 서버에 연결하도록 지원합니다. 직렬 장치 서버는 다음과 같이 tcp-server 모드에서 동작합니다. TCP 서버 모드에서 모듈은 로컬 포트를 모니터링하고 연결 요청이 전송되면 데이터 통신을 위한 연결을 수락하고 설정합니다. LAN 내에서 TCP 클라이언트와의 통신에 사용됩니다. LAN 에 서버가 없고 모듈에서 데이터를 요청하는 여러 컴퓨터 또는 휴대폰이 있는 시나리오에 적합합니다.

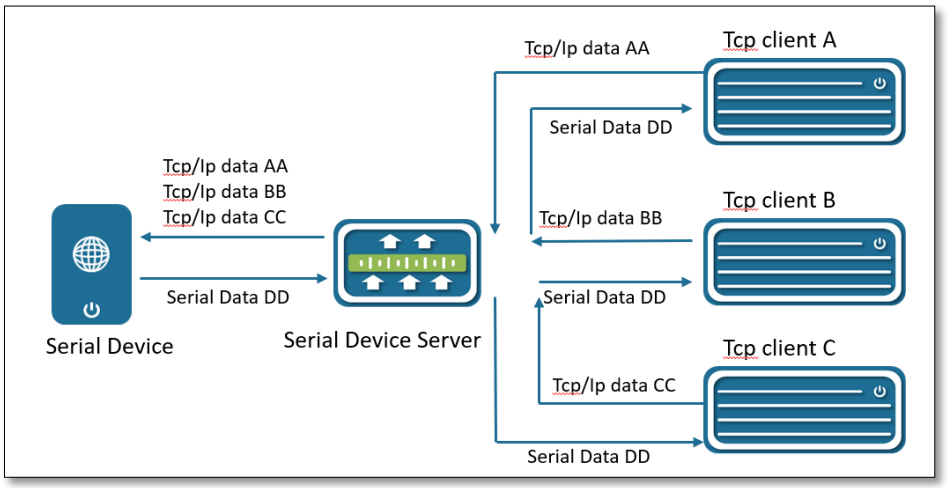


그림 3- 67 TCP 서버 모드에서 직렬 장치 서버 작동

3.7.1.2 시리얼 서버 설정

1. Configuration > Control > Serial Server 메뉴에서 Serial Server 페이지로 접속합니다.

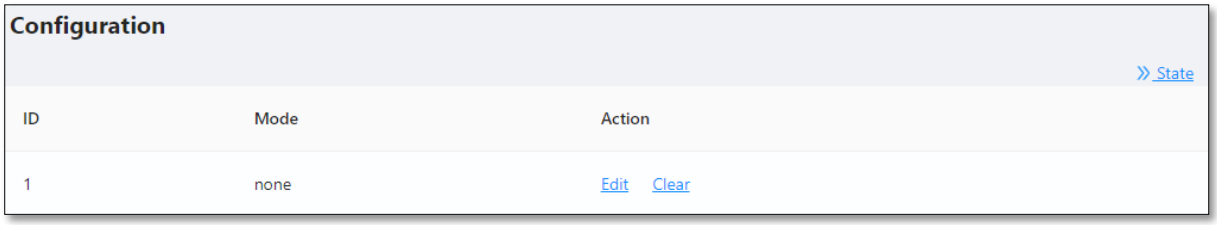


그림 3- 68 시리얼 서버 설정 요약

2. Edit 버튼을 클릭하여 서버 설정 메뉴로 접속합니다.

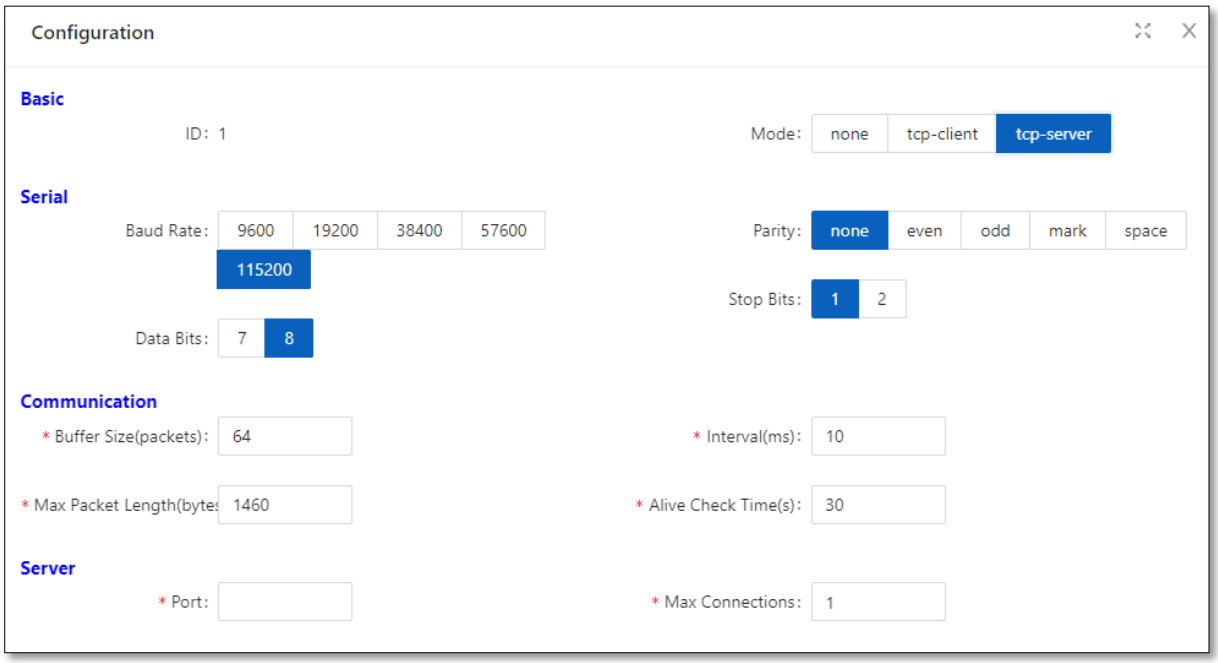


그림 3- 69 시리얼 서버 설정 메뉴

메뉴		설명
Basic	ID	직렬 포트 번호
Mode	None	직렬 포트 서버 종료
	tcp-client	작업 모드를 tcp-client 로 설정
	tcp-server	작업 모드를 tcp-server 로 설정
Serial	Baud Rate	직렬 포트의 전송 속도가 설정되며 9600, 19200, 38400, 57600 및 115200 의 5 가지 옵션이 있습니다.

	Data Bits	직렬 포트의 데이터 비트가 설정되며 7 과 8 의 두 가지 옵션이 있습니다.
	Parity	설정 체크 섬 방법에는 없음, 짝수, 홀수, 마크 및 공백의 5 가지 유형이 있습니다.
	Stop Bits	정지 비트 설정에는 1 과 2 의 두 가지 옵션이 있습니다.
Communication	Buffer size	직렬 포트 데이터 비트는 저속으로 전송되며 데이터는 네트워크 끝에서 직렬 포트 측으로 전송되어 전송 능력을 향상시킵니다. 범위는 <0-128>, 기본값은 64 입니다.
	Max packet Length	직렬 포트 데이터 패킷의 길이가 LEGGTH 값을 초과하면 패킷이 네트워크 끝으로 전달됩니다. 범위는 <0-1460>이며 기본값은 1460 입니다.
	Interval	직렬 포트 데이터 전후의 바이트 간격이 MILLISECONDS 를 초과하면 포스트 바이트 데이터가 새 메시지 헤더 바이트로 인식됩니다. 범위 < 1-1000 >, 기본값은 10ms 입니다.
	Alive check time	데이터 상호 작용이 없는 동안 활성 상태를 유지하도록 직렬 포트 서버를 설정한 다음 활성 감지가 시작됩니다.
Client	Remote IP	원격 연결 IP 주소 설정
	Remote port	<1-65535> 범위에서 원격 연결을 위한 포트 번호를 설정합니다.
	Local port	선택적 설정의 경우 기본 시스템이 자동으로 할당됩니다.
Server	Port	<1-65535 범위>의 tcp-server 포트 번호를 설정합니다.
	Max connections	1~65535 범위의 TCP 서버 모드의 최대 연결 수

표 3- 27 시리얼 서버 메뉴

3.7.2 IO Control

IO 제어 모듈은 DI, DO 두 부분으로 구분됩니다. 현재 소프트웨어에서 DO 는 그림과 같이 간단한 수동 제어 릴레이(DO) ON/OFF 전환 기능만 지원합니다. DI 는 그림에 표시된 대로 입력 레벨의 높고 낮음 판단만 지원합니다.

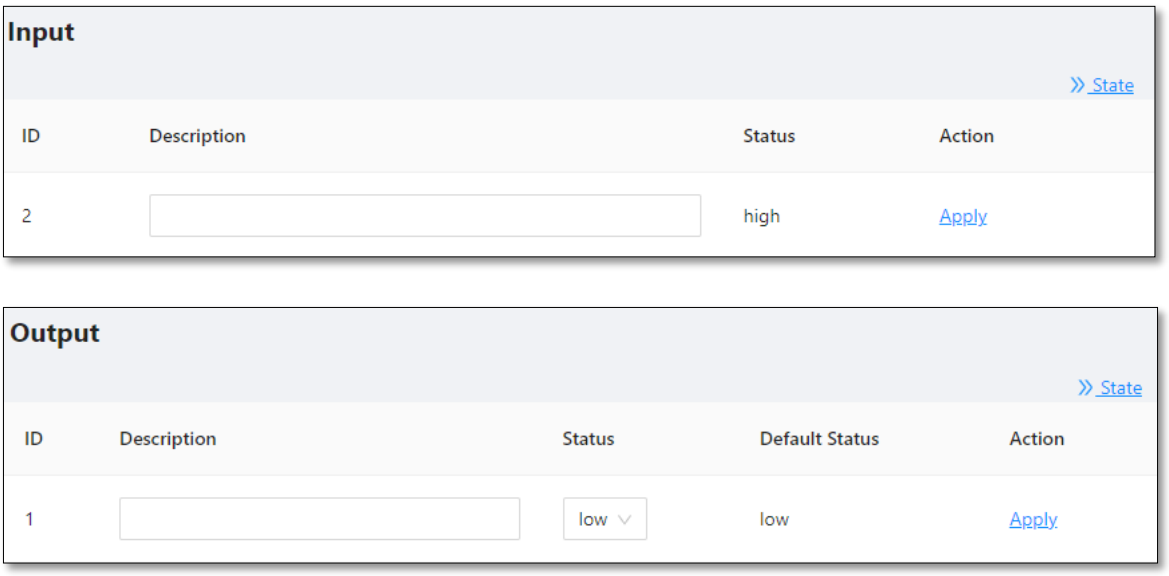


그림 3- 70 DI/DO 설정

3.8 LoopDetct

3.8.1 개요

LOOP-DETECT 는 다운링크 인터페이스에서 루프 오류를 신속하게 감지하는 데 사용되는 이더넷 루프 감지 프로토콜입니다. 오류가 발견되면 LOOP-DETECT 는 정상적인 데이터 교환에 영향을 미치지 않도록 사용자가 설정한 오류 처리 방법에 따라 관련 포트를 수동으로 닫거나 자동으로 닫도록 사용자에게 알립니다.

활성화 제어: 활성화 제어는 전역 활성화 제어와 포트 활성화 제어로 구분됩니다. 전역 활성화 제어가 활성화되고 포트에서 루프 감지가 활성화되면 포트는 루프 감지 기능을 지원합니다.

루프 동작: 포트에서 루프 오류가 감지되면 기본적으로 루프 오류를 수동으로 처리하라는 알림이 사용자에게 표시되며 포트 자동 닫기도 설정할 수 있습니다. 포트가 자동으로 종료되면 포트는 시간 초과, 종료/종료 포트 없음, 복구 명령 또는 장치 재시작을 기다리면서 오류로부터 복구될 수 있습니다.

VLAN 지정: 기본적으로 포트 VLAN 속성은 무시됩니다. 특정 VLAN 도메인에서 루프 오류가 발생하는지 여부를 감지해야 하는 경우 포트에서 지정된 VLAN 을 설정하고 이 VLAN 도메인에 루프 데이터 경로가 있는지 여부만 감지할 수 있습니다.

장치는 기본적으로 비활성화되어 있는 snmp 서버에 대한 루프 오류 경보 및 루프 오류 복구 메시지 트랩을 지원합니다.

1. . Configuration > LoopDetect 메뉴에서 설정화면에 접속합니다. 이 페이지는 "Global Configuration" , "Port Configuration" 두가지 설명 화면으로 나뉩니다.
2. Global Configuration 페이지에서 루프 감지 스위치를 켜고 감지 간격을 설정 후 구성버튼을 클릭합니다.

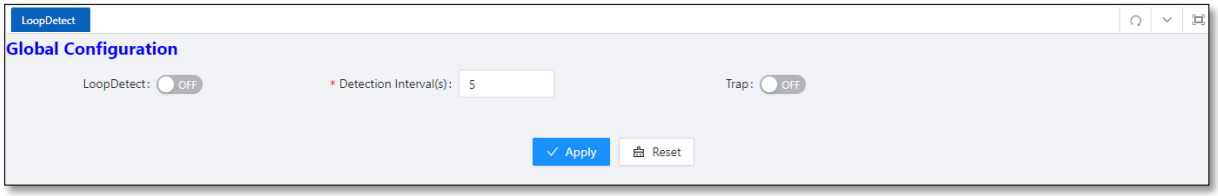


그림 3- 71 Loop protect Global 설정

메뉴	설명
Loop detection	루프 감지 기능을 켜거나 끕니다. 기본값은 전역적으로 포트를 끄는 것입니다.
Detection interval	루프 감지 간격 설정(범위 5~300 초, 기본값 5 초)
Trap	루프 오류 트랩 경보 활성화/비활성화

표 3- 28 Loop protect 설정 메뉴

3. Batch Edit 버튼을 클릭합니다. "Port Configuration" 페이지에 접속합니다.

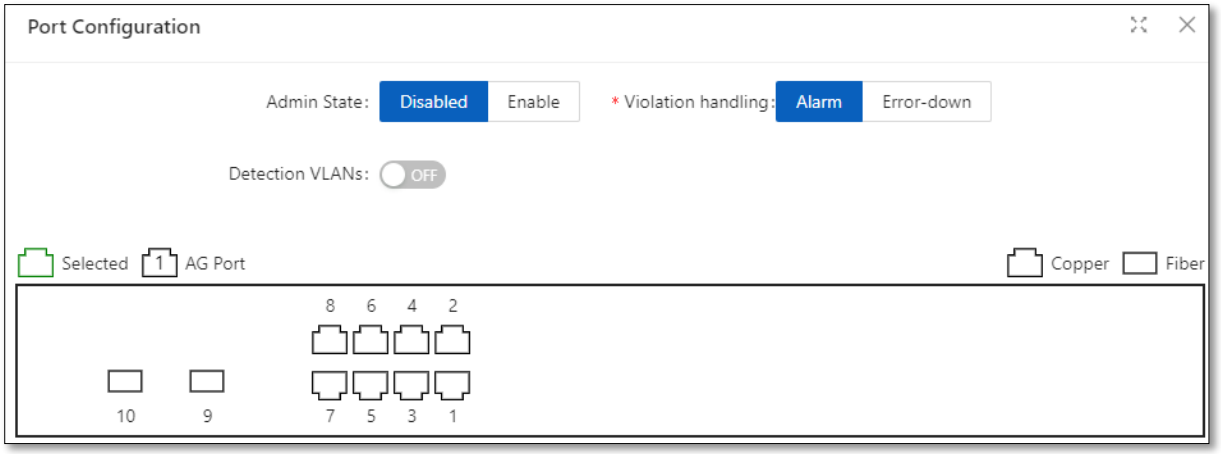


그림 3- 72Loop protect 포트 설정

메뉴	설명
Admin State	활성화: 포트의 루프 감지 기능을 활성화합니다. 비활성화됨: 포트의 루프 감지 기능을 끕니다.
Violation handling	경보: 루프 발생 시 트랩 경보 오류 다운: 루프가 발생하면 루프 포트를 종료합니다.
Detection VLANs	지정된 VLAN 도메인 내에서 데이터 경로 루프가 발생하는지 감지

4. Advance

4.1 LLDP

4.1.1 개요

네트워크에서 다양한 공급업체 유형의 네트워크 장치가 서로를 검색하고 설정을 교환할 수 있도록 보장합니다. LLDP(링크 계층 검색 프로토콜)는 IEEE 802.1AB 에 지정되어 있습니다. 프로토콜은 데이터 링크 계층에서 동작하여 직접 연결된 장치 간에 장치 정보를 교환합니다. LLDP 를 사용하면 장치는 로컬 장치 정보를 LLDPDU(LLDP 데이터 단위)의 TLV(유형, 길이 및 값) 삼중항으로 직접 연결된 장치에 보냅니다. 로컬 장치 정보에는 시스템 기능, 관리 IP 주소, 장치 ID, 포트 ID 등이 포함됩니다. 장치는 표준 MIB 의 LLDP 이웃에서 가져온 LLDPDU 에 장치 정보를 저장합니다. LLDP 를 사용하면 네트워크 관리 시스템이 레이어 2 네트워크 토폴로지 변경 사항을 신속하게 감지하고 식별할 수 있습니다.

NOTE:

- PoE 관련 구간에 대한 TLV 는 지원하지 않습니다.

4.1.2 LLDP 설정

- LLDP Global 설정

1. Advance > Layer2 > LLDP Configuration 메뉴에서 Global Configuration 페이지로 접속합니다.
2. Enable 버튼을 클릭하여 상태를 활성화합니다.
3. "System Name" 과 "Description"을 입력합니다.
4. 설정을 적용하려면 Apply 버튼을 클릭합니다.

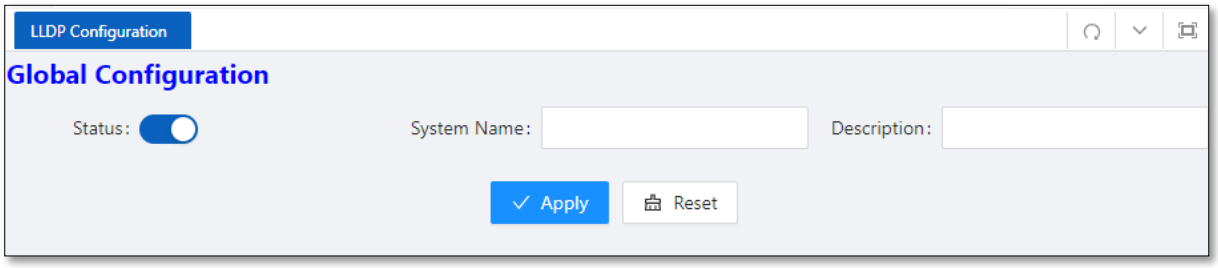


그림 4- 1 LLDP Global 설정

메뉴	설명
Status	Disabled: 비활성화 Enabled: 활성화
System Name	장치 이름은 비워둘 수 있습니다.
Description	시스템 설명, 비어 있을 수 있습니다.
Apply	설정을 적용하려면 클릭합니다.

표 4- 1 LLDP Global 메뉴

- LLDP 포트 설정

1. LLDP Global 설정이 활성화되면 포트 설정 페이지가 활성화됩니다.

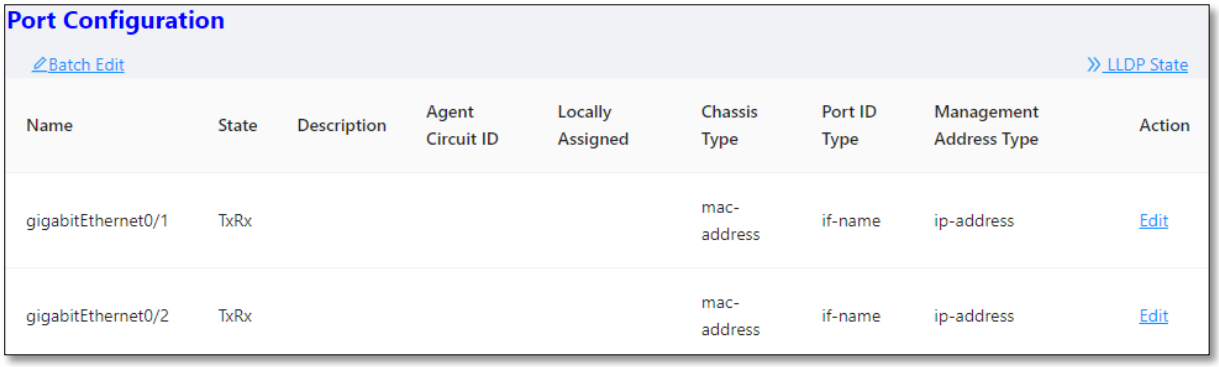


그림 4- 2 LLP 포트 설정 상태

2. "port configuration" 아래의 Batch Edit 버튼을 클릭하고 포트에 해당하는 편집 버튼을 클릭하여 설정페이지로 접속합니다.

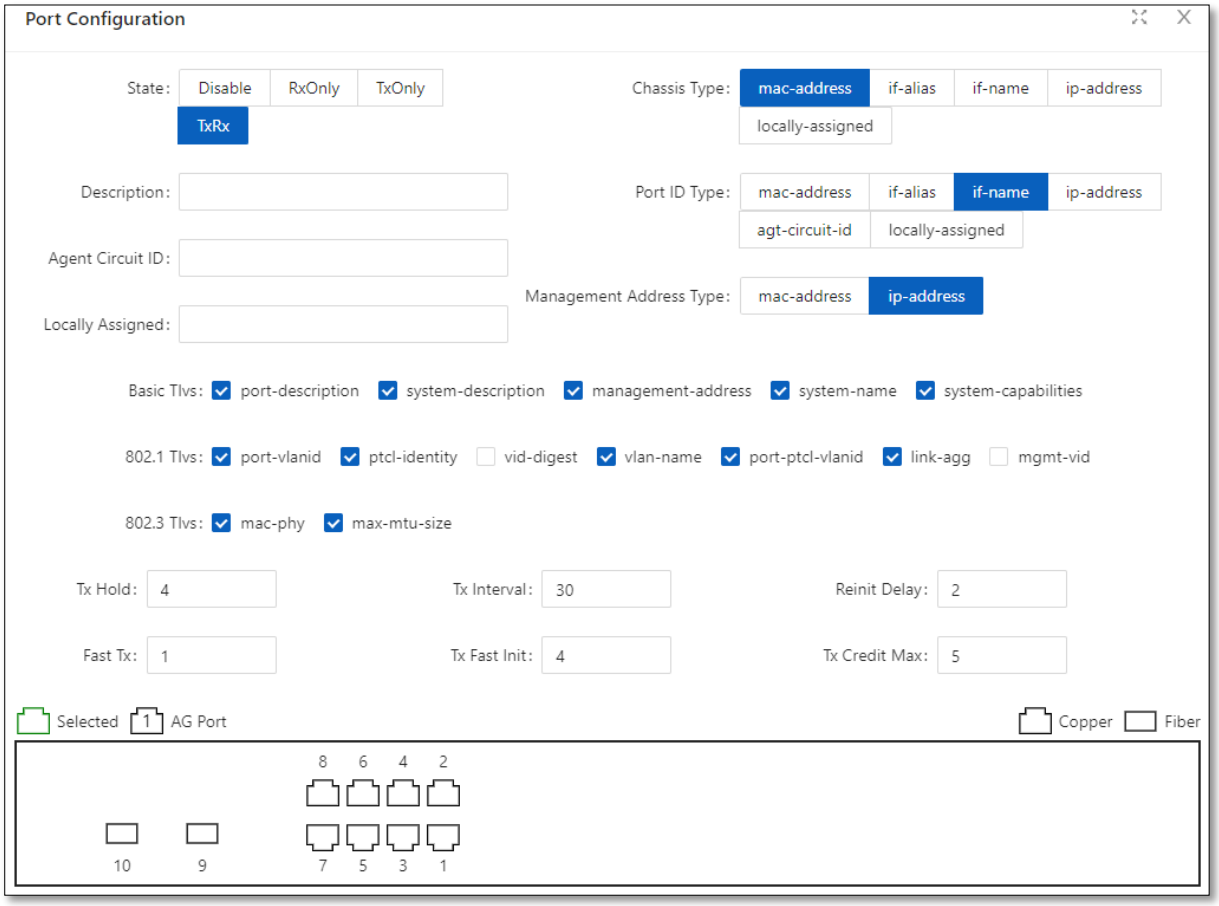


그림 4- 3 LLDP 포트 설정 상태

메뉴	설명
Description	현재 설정된 LLDP 포트에 대한 설명
Agent Circuit ID	에이전트 회로 식별. port-id-tlv 의 값으로 사용할 수 있습니다.
Locally Assigned	로컬로 할당됨
Admin Status	Disabled: LLDP 패킷이 인터페이스에서 전송/수신되지 않습니다. TxOnly: LLDP 패킷이 인터페이스에서 전송됩니다. RxOnly: LLDP 패킷이 인터페이스에서 수신됨 TxRx: LLDP 패킷이 인터페이스에서 전송/수신됩니다.
Chassis Subtype	Mac-address:MAC 주소 If-alias: 인터페이스 별칭을 나타냅니다. If-name: 인터페이스 이름을 나타냅니다. Ip-address: IP 주소 Locally-assigned: 로컬 설정을 나타냅니다.
Port ID Subtype	Mac-address:MAC 주소 If-alias: 인터페이스 별칭을 나타냅니다. If-name: 인터페이스 이름을 나타냅니다. Ip-address: IP 주소 Agt -circuit-id: agt-circuit-id 를 나타냅니다 Locally-assigned: 할당된 로컬을 나타냅니다.
Management Address Subtype	Mac-address: 장치 MAC 주소 Ip-address: 장치 IP 주소
Basic Tlvs	port-description : 포트 설명 system-description: 시스템 설명 management-address: 관리 주소 system-name: 시스템 이름 system-capabilities: 시스템 기능
802.1 Tlvs	port-vlanid: 포트의 VLAN ID ptcl -ID: 프로토콜 ID vid-digest: 비디오 다이제스트 vlan-name: VLAN 이름 port-ptcl - vlanid: 포트 프로토콜 vlanid link- agg mgmt -vid: 링크 집합 관리 영상
802.3 Tlvs	mac-phy: 포트에서 지원하는 속도 및 이중 상태, 포트 속도 자동 협상 지원 여부, 자동 협상 기능 활성화 여부, 현재 속도 및 이중 상태 max - mtu - 크기: 최대 MTU 값

Tx hold	전송 보류,기본값 txFastInit 은 4 입니다. 패킷 TTL 계산에 사용됩니다. TTL=msgTxInterval * msgTxHold + 1
Tx interval	환승 간격,기본값은 30 초입니다. 관리자는 이 값을 다음 사이의 값으로 변경할 수 있습니다. 5 ~ 300 초.
Reinit delay	다음 시점 사이의 지연 정도를 나타냅니다.adminStatus 는 'disable' 상태가 되고 재초기화를 시도하면 됩니다. reinitDelay 의 기본값은 2 초입니다.
Description	빠른 전송 기간 내에서 두 전송 사이의 타이머 간격에 대한 시간 간격을 정의합니다(예:TX Fast 는 0 이 아닙니다). Fast Tx 의 기본값은 1 입니다. 관리자는 이 값을 1 에서 3600 사이의 값으로 변경할 수 있습니다.
Agent Circuit ID	이 변수는 다음과 같이 사용됩니다. TX Fast 변수의 초기값. 이 값은 빠른 전송 기간 동안 전송되는 LLDPDU 수를 결정합니다.
Locally Assigned	최대값을 설정합니다. TX Credit. 기본값은 5 입니다. 관리자는 이 값을 1~10 범위의 값으로 변경할 수 있습니다.

표 4- 2 LLDP 포트 상태 메뉴

- LLDP 상태 보기

1. 페이지 오른쪽의 LLDP State 버튼을 클릭하여 LLDP 상태 페이지로 접속합니다.

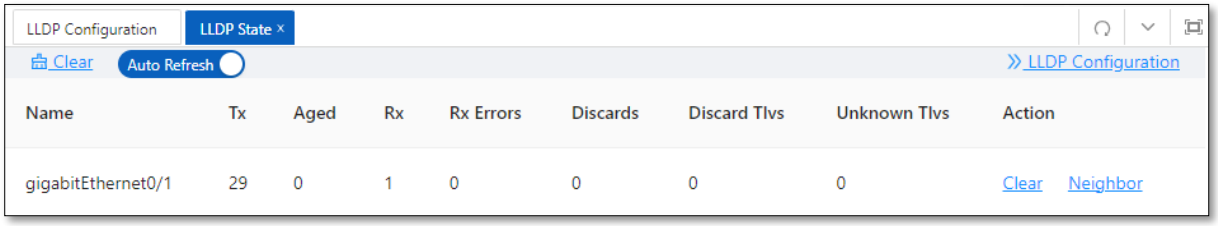


그림 4- 4 LLDP 포트 통계

메뉴	설명
Name	현재 설정된 LLDP 포트에 대한 설명
Tx	인터페이스에서 전송된 패킷 수
Aged	인터페이스에서 에이징된 패킷 수
Rx	인터페이스에서 수신된 패킷 수
Rx Errors	인터페이스에서 수신된 오류 패킷 수
Discards	인터페이스에서 폐기된 패킷 수
Discard Tlvs	인터페이스에서 폐기된 tlv 패킷 수
Unknown Tlvs	인터페이스의 알 수 없는 tvs 패킷 수

CLEAR	현재 인터페이스에서 카운터 지우기

표 4- 3 LLDP 포트 설정 메뉴

- LLDP neighbor 정보 보기

1. 현재 LLDP 상태 페이지에서 해당 포트의 'Neighbor' 버튼을 클릭하여 페이지에 접속합니다.

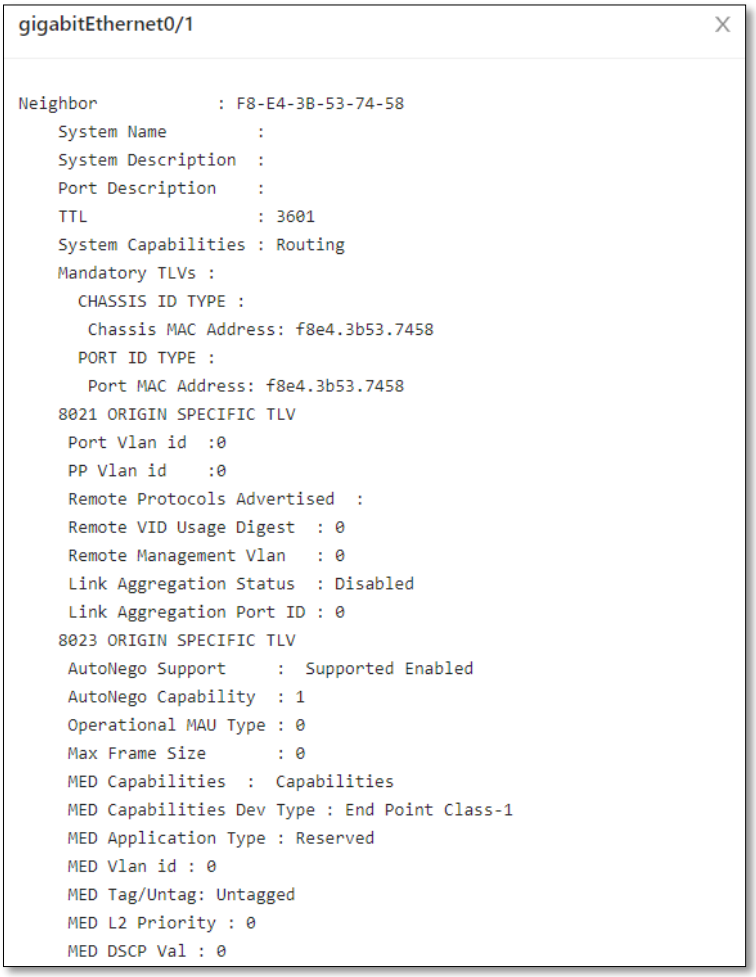


그림 4- 5 LLDP Neighbor 정보 보기

4.2 IGMP Snooping

4.2.1 IGMP Snooping 의 원리

IGMP 스누핑(Internet Group Management Protocol Snooping)은 멀티캐스트 그룹을 관리하고 제어하기 위해 레이어 2 에서 실행되는 멀티캐스트 제한 메커니즘입니다.

IGMP 스누핑을 실행하는 레이어 2 장치는 수신된 IGMP 메시지를 분석하여 포트와 멀티캐스트 MAC 주소 간의 매핑을 설정하고 이러한 매핑을 기반으로 멀티캐스트 데이터를 전달합니다. 표시된 바와 같이 IGMP 스누핑이 스위치에서 실행되지 않는 경우 멀티캐스트 패킷은 계층 2 의 모든 장치로 플러딩 됩니다. 그러나 IGMP 스누핑이 스위치에서 실행 중인 경우 알려진 멀티캐스트 그룹에 대한 멀티캐스트 패킷은 모든 장치에 브로드캐스트되는 대신 수신기에 멀티캐스트 됩니다.

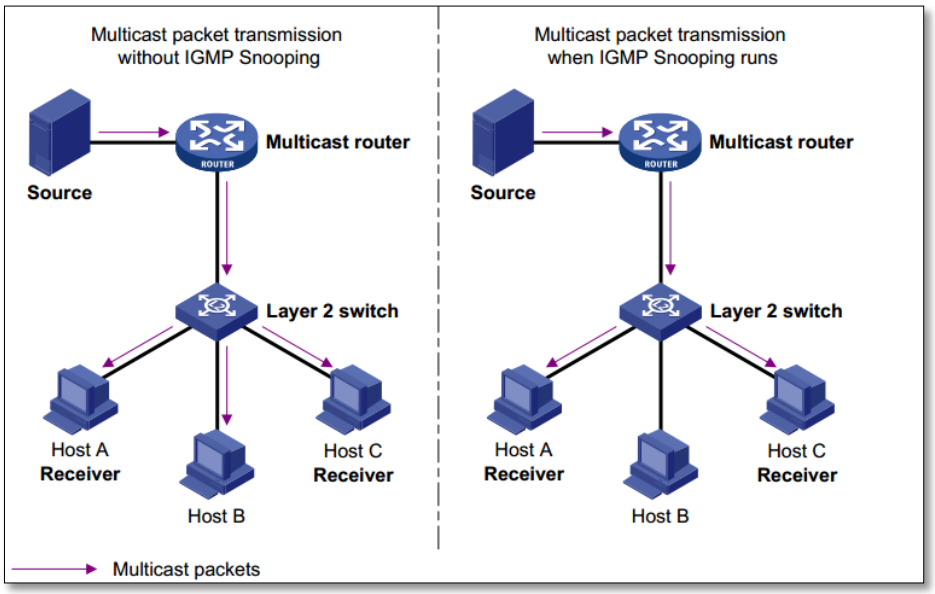


그림 4- 6 IGMP 스누핑의 원리

4.2.2 IGMP Snooping 설정

4.2.2.1 Global 설정

1. Advance > Layer2 > IGMP Snooping Configuration 메뉴에서 Global Configuration 페이지로 접속합니다.

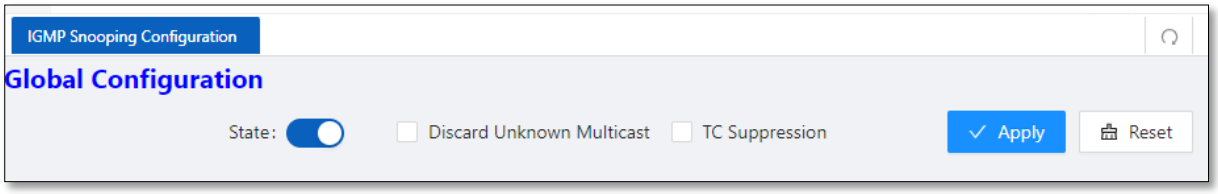


그림 4- 7 IGMP global 설정

메뉴		설명
Global Configuration	State	비활성화: 글로벌 비활성화 활성화: 글로벌 활성화
	Discard Unknown Multicast	이 옵션을 활성화하면 알 수 없는 멀티캐스트 트래픽이 스위치에 의해 삭제됩니다.
	TC Suppression	이 옵션이 활성화되면 토폴로지 변경 이벤트가 스위치에 의해 무시됩니다.

표 4- 4 IGMP M-Router 인터페이스 메뉴

4.2.2.2 IGMP M-router 인터페이스 구성

1. Advance > Layer2 > IGMP Snooping Configuration 을 선택하여 그림 4-8 과 같이 IGMP M-라우터 인터페이스 섹션으로 들어갑니다. 표 4-5 는 IGMP M-라우터 인터페이스 구성 항목을 설명합니다.

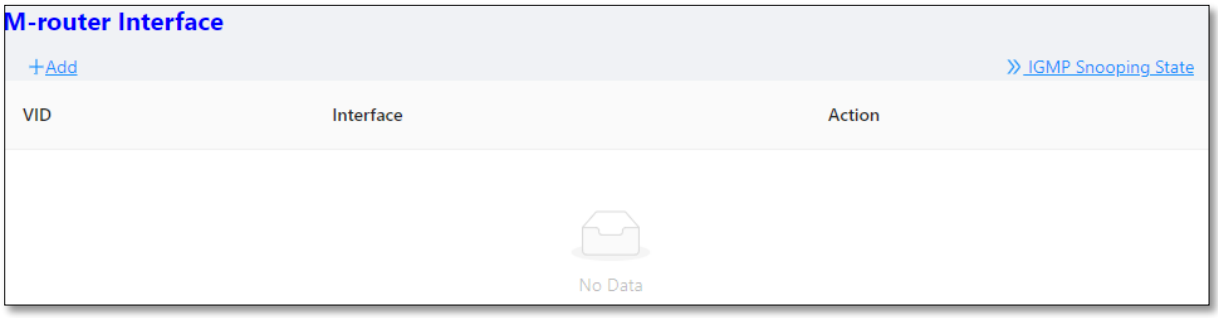


그림 4- 8 M-router 인터페이스

메뉴		설명
IGMP Router Interface	VID	VLAN ID
	Interface	인터페이스 이름.
	Delete	이 메뉴를 삭제하려면 클릭하세요.

표 4- 5 IGMP M-Router 인터페이스 메뉴

2. 그림 4-9 와 같이 IGMP M-라우터 인터페이스를 생성하려면 +추가 버튼을 클릭합니다. VID 와 인터페이스를 구성한 다음 확인을 클릭합니다.



그림 4- 9 IGMP-M-router 생성

4.2.2.3 IGMP Static 그룹 설정

1. Advance > Layer2 > IGMP Snooping Configuration 메뉴에서 IGMP Static Group 페이지로 접속합니다.

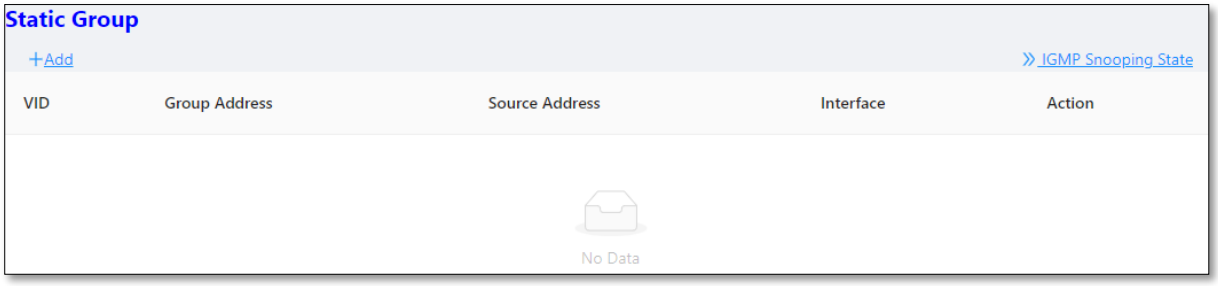


그림 4- 10 IGMP Static 그룹

메뉴		설명
IGMP Static Group	VID	VLAN ID
	Group Address	그룹 IP 주소
	Source Address	소스 IP 주소
	Interface	인터페이스 이름.
	Delete	이 메뉴를 삭제하려면 클릭하세요.

표 4- 6 IGMP Static 그룹 메뉴

2. +Add 버튼을 클릭하여 IGMP Static 그룹을 생성합니다. 'Vid', 'Group Address', 'Source Address', 'Interface'를 생성하고 OK 버튼을 클릭합니다.



그림 4- 11 IGMP Static 그룹 생성

4.3 MAC Management

4.3.1 개요

프레임 전달을 위해 MAC 주소 테이블을 유지합니다. 이 테이블의 각 메뉴는 연결된 장치의 MAC 주소, 이 장치가 연결된 인터페이스, 인터페이스가 속한 VLAN 을 나타냅니다. MAC 주소 테이블은 정적 및 동적이라는 두 가지 유형의 메뉴로 설정됩니다. 정적 메뉴는 수동으로 설정되며 만료되지 않습니다. 동적 메뉴는 수동으로 설정하거나 동적으로 학습할 수 있으며 만료됩니다. 장치는 다음 단계를 실행하면서 포트(예: 포트 A)로부터 프레임을 수신한 후 MAC 주소를 학습합니다.

1. Source MAC 주소에 대한 프레임을 확인합니다.
2. 주소에 해당하는 메뉴에 대한 MAC 주소 테이블을 조회하고 다음을 수행합니다.
    - MAC 주소에 대한 메뉴가 발견되면 해당 메뉴를 업데이트합니다.
    - MAC 주소가 포함된 메뉴가 없으면 MAC 주소와 수신 포트(포트 A)가 포함된 메뉴를 MAC 주소 테이블에 추가합니다.
3. MAC 주소(MAC-SOURCE)가 학습된 후 장치가 MAC-SOURCE 로 향하는 프레임을 수신하면 장치는 MAC 주소 테이블을 조회한 다음 포트 A 에서 프레임을 전달합니다. 프레임을 전달할 때 장치는 MAC 주소 테이블을 기반으로 다음 전달 모드를 채택합니다.
    - 유니캐스트 모드 : 대상 MAC 주소와 일치하는 메뉴가 있으면 장치는 해당 메뉴에 기록된 송신 포트에서 직접 프레임을 전달합니다.
    - 브로드캐스트 모드: 장치가 대상 주소가 모두 F 인 프레임을 수신하거나 대상 MAC 주소와 일치하는 메뉴가 없는 경우 장치는 수신 포트를 제외한 모든 포트에 프레임을 브로드캐스트 합니다.

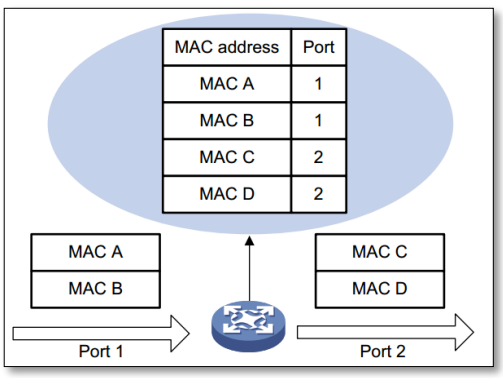


그림 4- 12 장치의 MAC 주소 테이블

4.3.2 MAC 주소 설정

MAC 주소 설정에는 수동 MAC 주소, 필터 MAC 주소 설정 및 표시, MAC 주소 메뉴 에이징 시간 설정이 포함됩니다.

- Global 설정

1. Advance > Layer2 > MAC Configuration 메뉴에서 MAC global Configuration 페이지로 접속합니다.



그림 4- 13 Global 설정 페이지

메뉴		설명
Global configuration	Aging time	MAC 주소의 에이징 시간을 설정합니다. 기본값은 300 초입니다.
	Apply	클릭하면 활성화됩니다.

표 4- 7 MAC Global 설정 메뉴

- Static MAC 주소 설정

1. Advance > Layer2 > MAC Configuration 메뉴에서 Static MAC Address Configuration 페이지로 접속합니다.

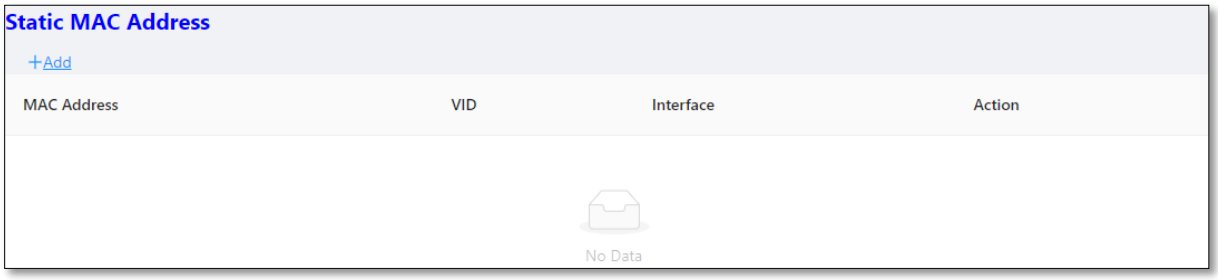


그림 4- 14 Static MAC 주소 설정

2. +ADD 버튼을 클릭하면 Static MAC 주소를 설정할 수 있습니다.

3. MAC 주소, VID, Interface 를 입력합니다.

4. OK 버튼을 클릭합니다.



그림 4- 15 Static MAC 주소 생성

메뉴		설명
Static Mac Address	MAC Address	추가할 MAC 주소를 설정합니다.
	VID	MAC 주소가 속한 VLAN 의 ID 를 설정합니다.
	Interface	MAC 주소가 속한 포트를 설정합니다.

표 4- 8 Static MAC 주소 메뉴

- MAC 필터 설정

1. Advance > Layer2 > MAC Configuration 메뉴에서 Filter MAC Address 페이지로 접속합니다.

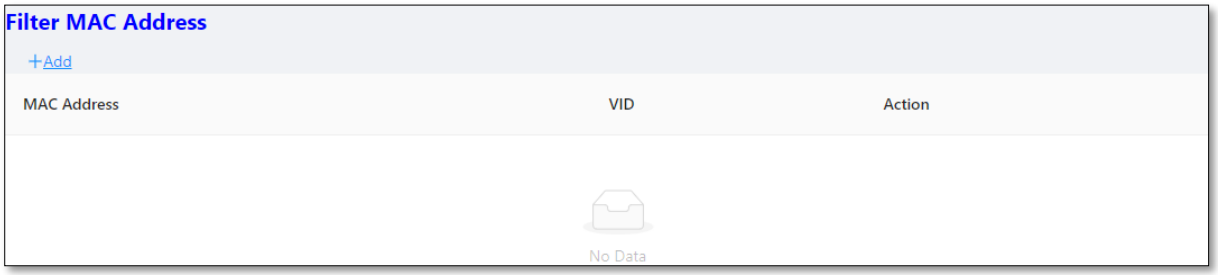


그림 4- 16 MAC 필터 설정 페이지

2. +ADD 를 클릭하면 필터 MAC 주소를 생성하는 페이지로 전환합니다.

3. MAC 주소, VID 를 입력합니다.

4. Apply 를 클릭하여 설정을 적용합니다.



그림 4- 17 필터 MAC 주소 설정

메뉴		설명
Static Mac Address	MAC Address	필터링할 MAC 주소를 설정합니다.
	VID	MAC 주소가 속한 VLAN 의 ID 를 설정합니다.

표 4- 9 필터 MAC 주소 메뉴

4.4 DHCP Snooping

4.4.1 개요

DHCP 스누핑(동적 호스트 설정 프로토콜)은 신뢰할 수 없는 호스트와 신뢰할 수 있는 DHCP 서버 사이에서 방화벽처럼 동작하는 보안 기능입니다. VLAN 에서 DHCP 스누핑이 활성화되면 시스템은 VLAN 과 연결된 신뢰할 수 없는 호스트에서 보낸 DHCP 메시지를 검사하고 해당 호스트의 IP 주소와 임대 정보를 추출합니다. 이 정보는 DHCP 스누핑 데이터베이스를 구축하고 유지하는 데 사용됩니다. DHCP 스누핑은 VLAN 별로 활성화됩니다. 기본적으로 이 기능은 모든 VLAN 에서 비활성화되어 있습니다. 단일 VLAN 또는 다양한 VLAN 에서 이 기능을 활성화할 수 있습니다.

- 신뢰할 수 있는 Source

DHCP 스누핑 기능은 트래픽 소스를 신뢰할 수 있는지 여부를 결정합니다. DHCP 스누핑은 신뢰할 수 있는 DHCP 서버에 의해 다운스트림 네트워크 장치에 할당된 유효한 IP 주소를 추적하여 네트워크 보안의 수호자 역할을 합니다. 모든 인터페이스의 기본 신뢰 상태는 신뢰할 수 없음입니다.

- DHCP Snooping Limit Rate

인터페이스가 수신할 수 있는 초당 DHCP 패킷 수를 설정하여 이 인터페이스에서 DHCP 패킷 공격의 영향을 줄이거나 제거합니다.

- MAC 주소 확인

DHCP 스누핑 MAC 주소 확인이 활성화되면 DHCP 스누핑은 신뢰할 수 없는 포트에서 수신된 DHCP 패킷에서 소스 MAC 주소와 클라이언트 하드웨어 주소가 일치하는지 확인합니다. 소스 MAC 주소는 패킷과 관련된 계층 2 필드이고 클라이언트 하드웨어 주소는 DHCP 패킷의 계층 3 필드입니다.

- Option-82

DHCP Option82 옵션은 여러 DHCP 옵션 중 하나인 DHCP Relay Agent 정보 옵션이라고도 합니다. Option82 옵션은 DHCP 서버의 보안을 강화하고 IP 주소 할당 전략을 개선하기 위해 제안된 DHCP 옵션입니다. 옵션 추가 및 제거는 릴레이 설정요소에 의해 구현됩니다.

- DHCP 데이터베이스

DHCP 스누핑 기능은 가로채는 DHCP 메시지에서 추출된 정보를 사용하여 데이터베이스를 동적으로 구축하고 유지 관리합니다. 호스트가 DHCP 스누핑이 활성화된 VLAN 과 연결된 경우

데이터베이스에는 임대된 IP 주소가 있는 신뢰할 수 없는 각 호스트에 대한 메뉴가 포함되어 있습니다. 데이터베이스에는 신뢰할 수 있는 인터페이스를 통해 연결된 호스트에 대한 메뉴가 포함되어 있지 않습니다. 인터페이스에서 IP 확인 소스 기능이 활성화되면 데이터베이스 메뉴가 인터페이스에서 유효한 사용자로 동작합니다.

4.4.2 DHCP Snooping 설정

- Global DHCP Snooping 설정

1. Advance > Layer2 > DHCP Snooping 메뉴에서 DHCP Snooping Configuration 페이지로 접속합니다.

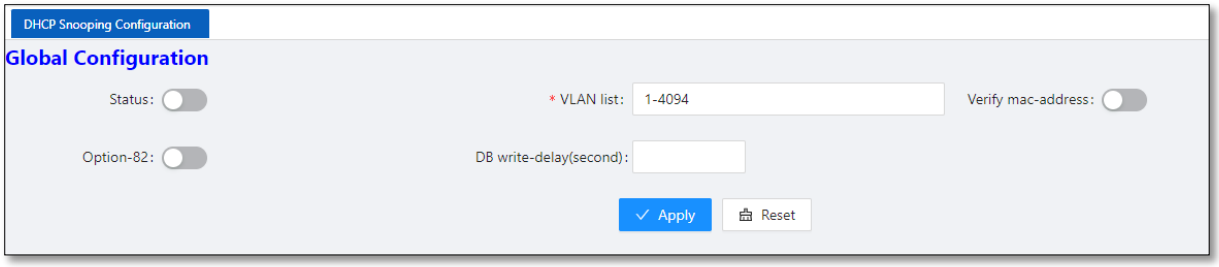


그림 4- 18 DHCP Snooping Global 설정

메뉴	설명
Status	DHCP 스누핑을 전역적으로 활성화/비활성화합니다.
Vlan	VLAN 에서 DHCP 스누핑을 활성화/비활성화합니다.
Verify mac-address	소스 MAC 주소와 클라이언트 하드웨어 주소가 DHCP 패킷에서 일치하는지 확인하십시오.
option-82	옵션-82 삽입 활성화/비활성화
DB write-delay(s)	플래시에 기록하는 간격 시간 데이터베이스 구성

표 4- 10 DHCP Snooping 설정 메뉴

- DHCP Snooping Port 설정

1. Advance > Layer2 > DHCP Snooping 메뉴에 접속합니다.

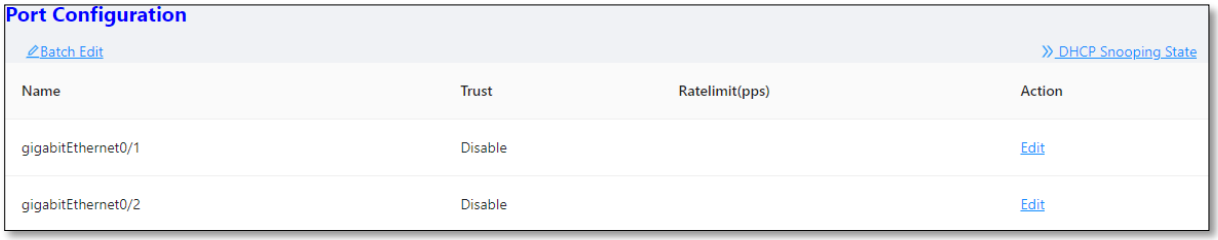


그림 4- 19 DHCP Snooping 인터페이스 설정 상태

2. "port configuration"을 클릭하거나 해당포트에 Edit 버튼을 클릭하여 설정 페이지로 접속합니다.

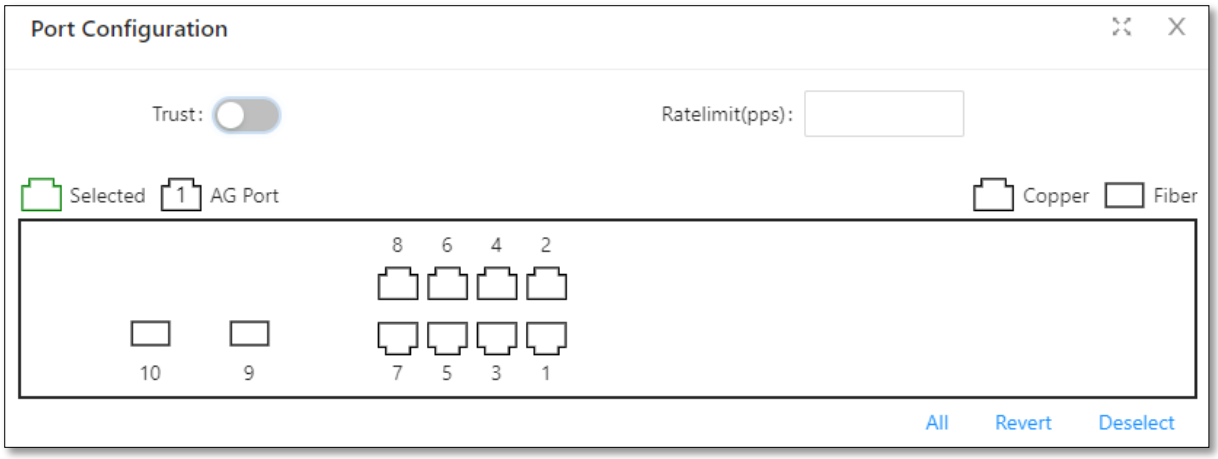


그림 4- 20 DHCP Snooping 포트 설정

메뉴	디비문
Trust	트래픽 소스를 신뢰할 수 있는지 여부를 결정합니다.
Ratelimit(pps)	인터페이스가 수신할 수 있는 초당 DHCP 패킷 수 설정

표 4- 11 DHCP Snooping 인터페이스 설정 메뉴

NOTE:

- 하드웨어 제한으로 인해 DHCP 속도 제한의 경우 제한 값이 0 이 아닌 경우 소프트웨어 속도 제한이 사용되고, 제한 값이 0 인 경우 하드웨어 속도 제한이 사용됩니다. 소프트웨어 속도 제한은 CPU 리소스를 소비합니다.

- DHCP Snooping 상태보기

1. DHCP Snooping state 버튼을 클릭하면 상태 보기 메뉴로 접속합니다.

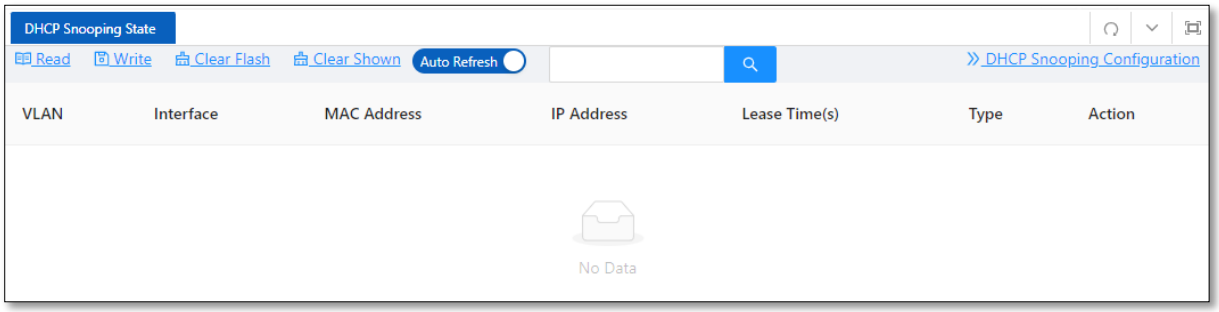


그림 4- 21 DHCP Snooping 상태보기

메뉴	디비문
Search	입력 문자열과 퍼지 일치하여 데이터베이스 메뉴 검색.
WRITE	플래시에 데이터베이스 메뉴 쓰기
READ	플래시에서 데이터베이스 메뉴 읽기
CLEAR	데이터베이스 메뉴를 지우고 키워드를 선택하여 범위를 좁힐 수 있습니다.

표 4- 12 DHCP Snooping 데이터베이스에 설명

4.5 QinQ

4.5.1 개요

QinQ 는 IEEE 802.1Q 를 기반으로 하는 유연하고 구현하기 쉬운 레이어 2 VPN 기술입니다. QinQ 를 사용하면 서비스 제공업체 네트워크의 Edge 장치가 고객 네트워크의 이더넷 프레임에 외부 VLAN 태그를 삽입할 수 있으므로 이더넷 프레임이 이중 VLAN 태그를 사용하여 서비스 제공업체 네트워크(공용 네트워크)를 통해 이동합니다. QinQ 를 사용하면 서비스 공급자가 단일 SVLAN 을 사용하여 여러 CVLAN 을 보유한 고객에게 서비스를 제공할 수 있습니다.

- 배경 및 이점

IEEE 802.1Q VLAN 태그는 VLAN ID 로 12 비트를 사용합니다. 장치는 최대 4094 개의 VLAN 을 지원합니다. 이는 실제 네트워크, 특히 MAN(Metropolitan Area Network)에서 사용자를 격리하기에는 충분하지 않습니다.

태그 된 프레임에 태그를 지정함으로써 QinQ 는 사용 가능한 VLAN 공간을 4094 에서 4094 × 4094 로 확장합니다. QinQ 는 다음과 같은 이점을 제공합니다.

- SVLAN 리소스에 대한 스트레스를 해제합니다.
- 고객이 SVLAN 과 충돌하지 않고 CVLAN 을 계획할 수 있도록 합니다.
- 소규모 MAN 또는 인트라넷을 위해 구현하기 쉬운 레이어 2 VPN 솔루션을 제공합니다.
- 서비스 제공업체가 서비스 제공업체 네트워크를 업그레이드할 때 고객은 VLAN 할당 체계를 변경하지 않고 유지할 수 있습니다.

4.5.2 QinQ 설정

- VPN 설정

1. Advance > Layer2 > QinQ configuration 설정 메뉴로 접속합니다.

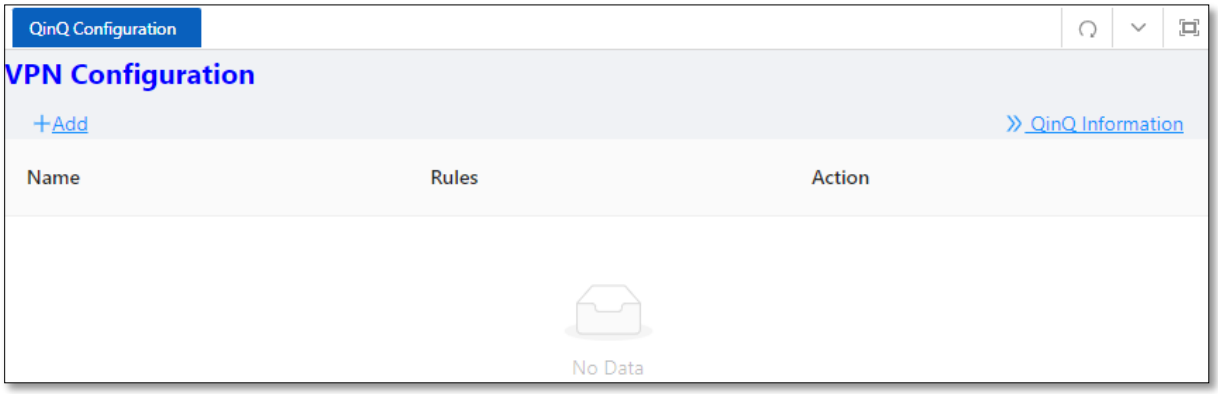


그림 4- 22 QinQ 설정

2. +ADD 버튼을 클릭하여 "VPN Configuration" 설정으로 접속합니다.



그림 4- 23 VPN 설정

메뉴	설명
Name	VLAN VPNRule 의 이름
CVID	고객 VLAN 의 ID
SVID	서비스 제공자 VLAN 의 ID

표 4- 13 VPN 설정 설명

- 포트 설정

1. Advance > Layer2 > QinQ configuration 설정 메뉴로 접속합니다.

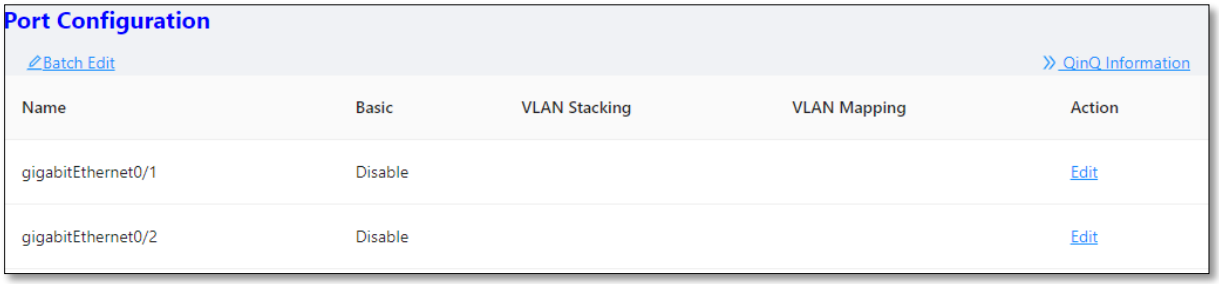


그림 4- 24 포트 설정 요약

2. +ADD 버튼을 클릭하거나 Edit 버튼을 클릭하여 QinQ 설정으로 접속합니다.

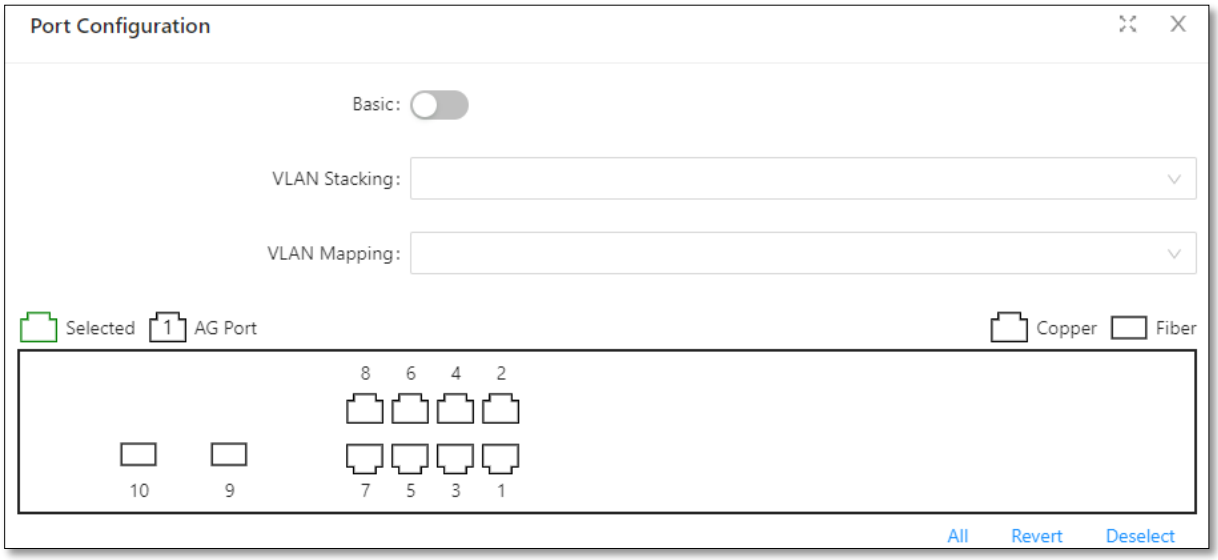


그림 4- 25 포트 설정

메뉴	설명
Basic	VLAN 매핑 모드 활성화
VLAN Stacking	다층 태그 모드
VLAN Mapping	태그 교체 모드

표 4- 14 QinQ 규칙 설정

4.6 ACL

4.6.1 개요

ACL(액세스 제어 목록)은 소스 IP 주소, 대상 IP 주소, 포트 번호 등의 기준에 따라 트래픽을 식별하기 위한 규칙 (또는 허용 또는 거부)입니다. ACL 은 기본적으로 패킷 필터링에 사용됩니다. 패킷 필터는 거부 규칙과 일치하는 패킷을 삭제하고 허용 규칙과 일치하는 패킷을 허용합니다. ACL 은 또한 트래픽 식별을 위해 QoS 및 IP 라우팅과 같은 많은 모듈에서 널리 사용됩니다.

4.6.2 ACL 설정

NOTE :

- 단일 ACL-ID 아래에 최대 128 개의 규칙을 구성할 수 있습니다. 하드웨어 리소스 제한으로 인해 단일 장치에서 지원하는 최대 애플리케이션 규칙 수는 특정 제품의 사양 문서를 참조하세요.
- ACL 이 포트에 적용된 경우 규칙을 추가하고 삭제해야 하는 경우 먼저 포트에서 해당 규칙을 적용 취소해야 합니다.

- IP ACL 에 대한 규칙 설정

1. Advance > Security > ACL Configuration 메뉴에 접속합니다.
2. +ADD 버튼을 클릭하여 규칙 설정 페이지로 접속합니다. 기본 ACL 에 대해 ACL 유형을 선택합니다.

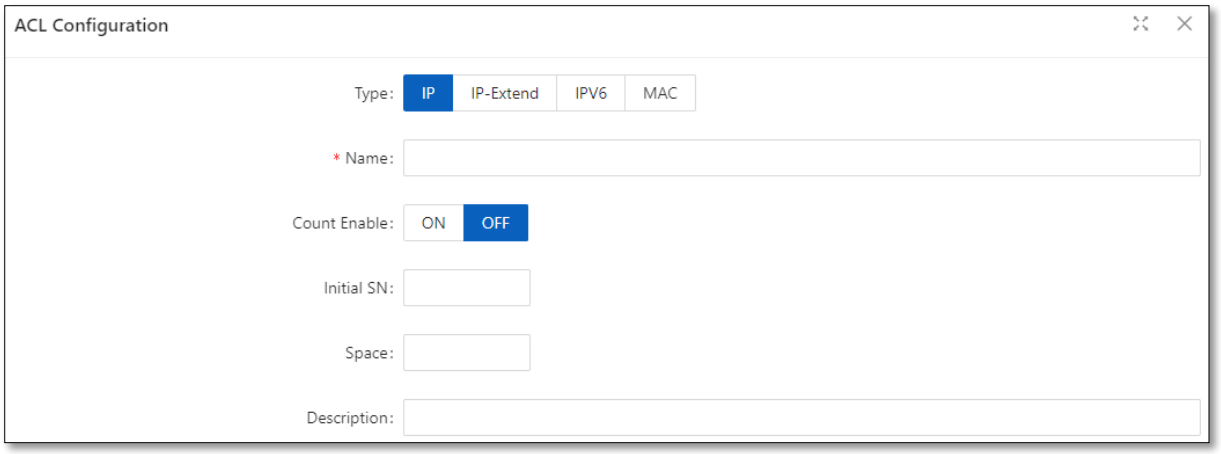


그림 4- 26 IP ACL 설정

메뉴		설정
ACL Type	IP	표준 IP ACL 은 IPv4 패킷의 소스 IP 필드와 일치할 수 있습니다.
	IP-Extend	프로토콜 번호, 소스 IP 주소, IPv4 패킷의 대상 IP 주소, 레이어 4 포트 번호 등
	IPV6	IPv6 ACL 은 IPv6 패킷 소스 IP 주소, 대상 IP 주소, 프로토콜 번호 등과 일치할 수 있습니다.
	MAC	대상 MAC 주소, 소스 MAC 주소, Etype 및 기타 필드와 일치할 수 있는 MAC ACL
Name		표준 IP 유효 번호 범위: <1-99> | <1300-1999> 확장 IP 유효번호 범위: <100-199> | <2000-2699> MAC ACL 유효 번호 범위: <200-699> IPv6 ACL 은 문자열 이름 지정만 지원합니다. 모든 ACL 은 문자열 이름 지정을 지원합니다. 문자열 길이 범위는 <1-64>입니다.
Count Enable		계산 기능을 활성화합니다. 패킷이 ACL 에 도달하면 카운트 값이 1 씩 증가합니다.
Initial SN		규칙 메뉴 시퀀스 번호의 시작 값, 기본값: 10, 범위 <1-2147483647>
Space		일련번호 증가, 기본값: 10, 범위 <1-2147483647>
Description		ACL 설명 정보 정의

표 4- 15 IP ACL 기본 메뉴 설명

3. IP ACL 에 대한 규칙을 구성하고 확인을 클릭합니다.

4. "ACE Configuration" 아래의 상자에서 IP 규칙을 선택하고 +Add ACE 버튼을 클릭하여 설정 페이지로 접속합니다.

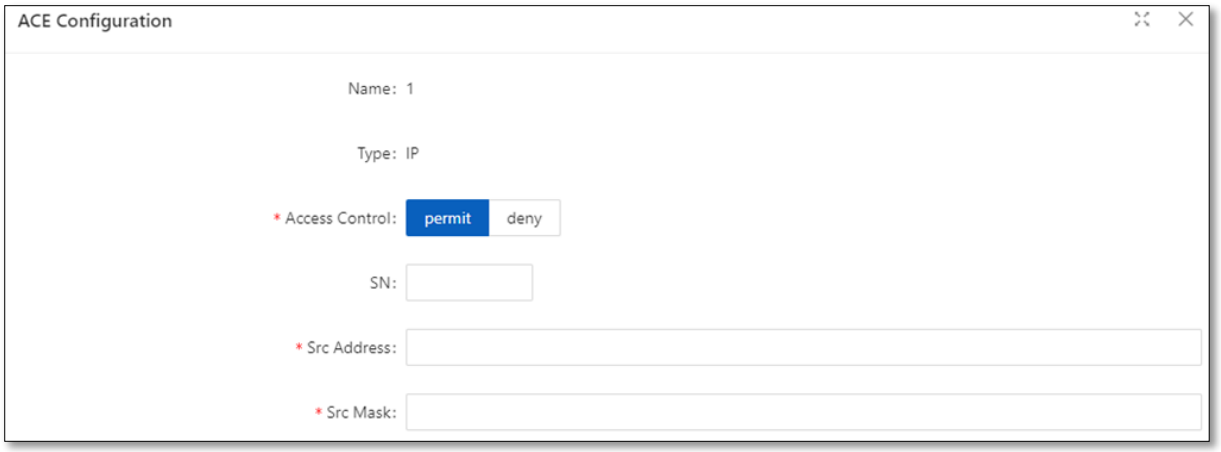


그림 4- 27 ACE 설정 인터페이스

나팀		디비문
Access Control	permit	이 규칙과 일치하는 패킷을 해제합니다.
	deny	이 규칙과 일치하는 패킷을 삭제합니다.
SN		규칙 메뉴 순서 번호
Src Address		소스 IP 주소(예: 192.168.64.1)
Src Mask		IP 마스크가 반전됩니다. IP 주소의 처음 24 자리와 일치하면 마스크는 255.255.255.0 입니다. 여기서는 00.00.00.255 로 구성해야 합니다.

표 4- 5 포트에 ACL 규칙 적용

5. ACE 를 구성하고 확인을 클릭합니다.

6. "Port Configuration" 아래 Batch Edit 를 클릭하여 ACL 포트 구성 페이지로 들어가서 해당 포트의 ACL 규칙을 선택한 다음 Ok 를 클릭합니다.

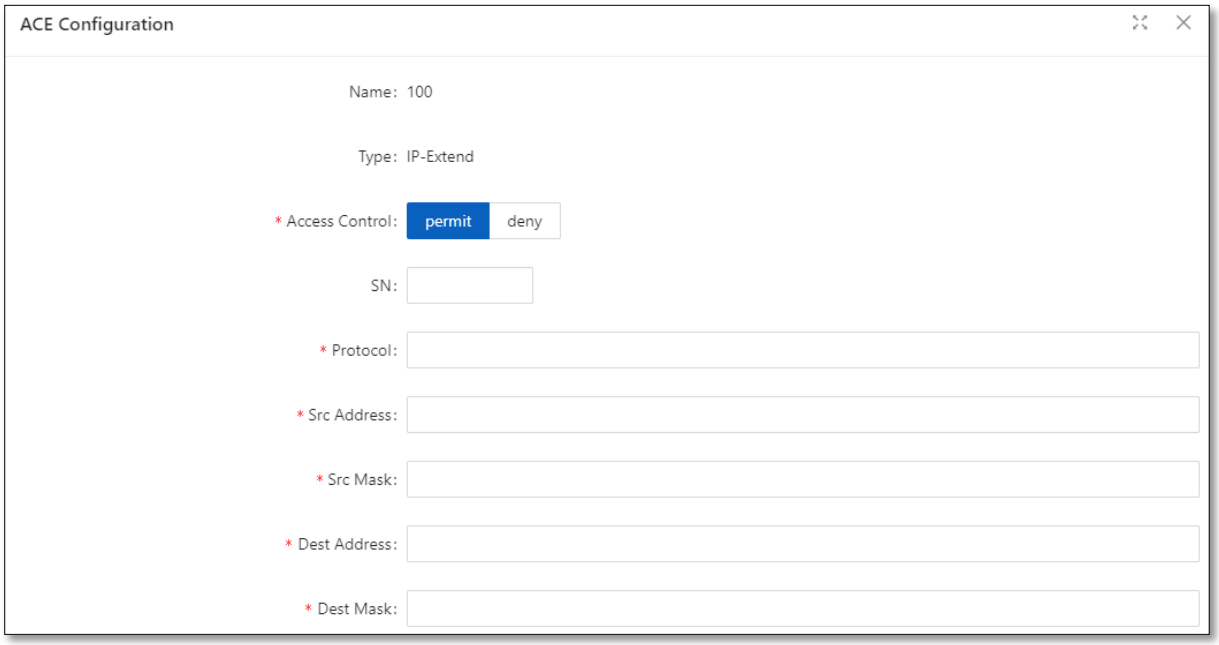


그림 4- 28 IP 확장형 ACE 구성 인터페이스

메뉴		설명
Access Control	permit	이 규칙과 일치하는 패킷을 해제합니다.
	deny	이 규칙과 일치하는 패킷을 삭제합니다.
SN		규칙 메뉴 순서 번호
Protocol		tcp, udp, vrrp, igmp, gre, ipcomp, ospf, pim, rsvp 등을 포함한 일반적인 프로토콜

	메시지 옵션을 지원합니다. 모든 IP v4 패킷 지원 맞춤형 프로토콜의 IPv4 메시지
Src Address	소스 IP 주소(예: 192.168.64.1)
Src Mask	IP 마스크가 반전됩니다. IP 주소의 처음 24 자리와 일치하면 마스크는 255.255.255.0 입니다. 여기서는 00.00.00.255 로 구성해야 합니다.
Dest Address	대상 IP 주소(예: 192.168.64.100)
Dest Mask	대상의 MASK

표 4- 67 IP 확장 ACL 에 대한 설명

7. ACE 를 설정하고 확인을 클릭합니다.

8. "Port Configuration"아래의 Batch 편집을 클릭하여 ACL 규칙을 선택하 후 OK 를 클릭합니다.

- IPV6 ACL 에 대한 규칙 설정

1. Select Advance > Security > ACL Configuration 메뉴에 접속합니다.

2. +ADD ACL 버튼을 클릭하여 규칙 구성 페이지로 들어가 그림과 같이 기본 ACL 에 대해 ACL 유형 'IPV6'을 선택합니다.

3. IP ACL 에 대한 규칙을 구성하고 확인을 클릭합니다.

4. "ACE Configuration" 아래 상자에서 ACL 규칙을 선택하고 +ACE 추가 버튼을 클릭하여 그림과 같이 ACE 구성 페이지로 들어갑니다.

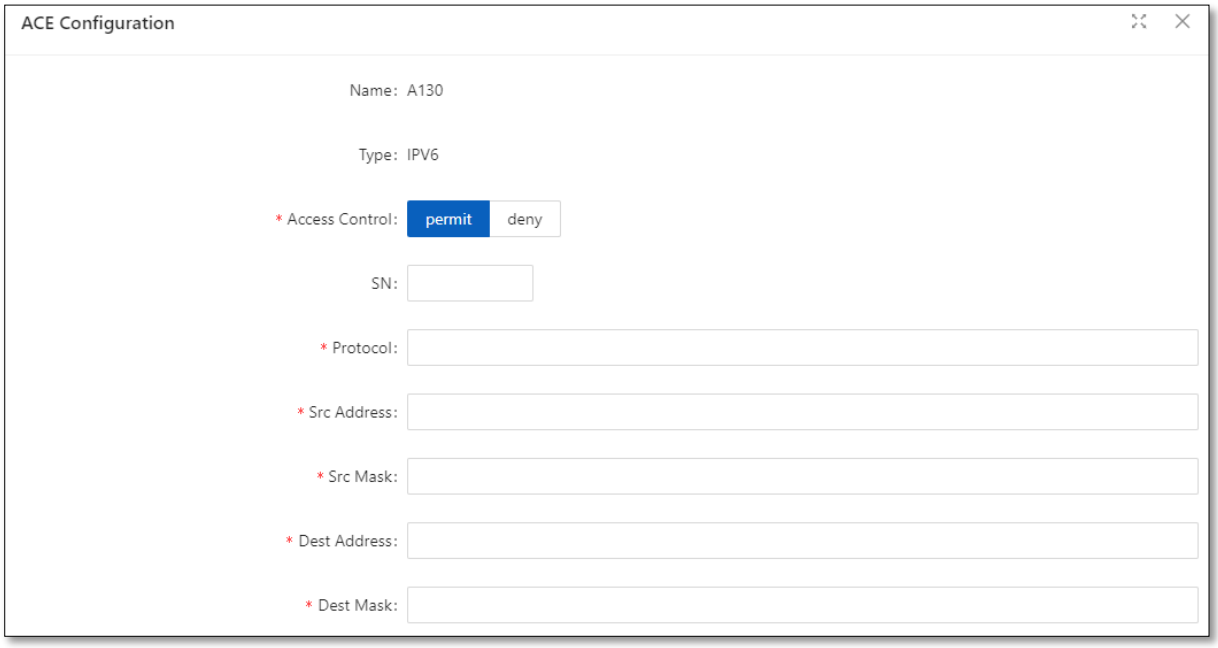


그림 4- 29 IPV6 유형 ACE 구성 인터페이스

메뉴		설명
Access Control	permit	이 규칙과 일치하는 패킷을 해제합니다.
	deny	이 규칙과 일치하는 패킷을 삭제합니다.
SN		규칙 메뉴 순서 번호
Protocol		tcp, udp, icmp 등을 포함한 일반적인 프로토콜 메시지 옵션을 지원합니다. 모든 IP v 6 패킷 지원 맞춤형 프로토콜의 IPv6 메시지 지원
Src Address		소스 MAC 주소(예: 00.d 0.f 8.22.33.40)
Src Mask		MAC 주소 마스크가 반전됩니다. MAC 주소의 처음 24 자리와 일치하면 마스크는 ffff.ff00.0000 입니다. 여기서는 0000.00 ff.ffff 로 구성해야 합니다.
Dest Address		대상 MAC 주소(예: 00.d 0.f 8.22.33.41)
Dest Mask		대상의 MASK

표 4- 7 IPV6 ACL 에 대한 설명

5. ACE 를 설정하고 확인을 클릭합니다.
6. "Port Configuration" 아래의 일괄 편집을 클릭하여 ACL 포트 구성 페이지로 들어가서 해당 포트의 ACL 규칙을 선택한 후 확인을 클릭합니다.

• MAC ACL 에 대한 규칙 설정

1. Advance > Security > ACL Configuration 메뉴에 접속합니다.
2. +ADD ACL 버튼을 클릭하여 규칙 설정 페이지로 접속합니다. 그림과 같이 기본 ACL 에 대해 ACL 유형 'IPV6'을 선택합니다.
3. IP ACL 에 대한 규칙을 구성하고 확인을 클릭합니다.
4. "ACE Configuration" 아래 상자에서 ACK 규칙을 선택하고 +Add ACE 버튼을 클릭하면 그림과 같이 ACE 구성 페이지로 접속합니다.

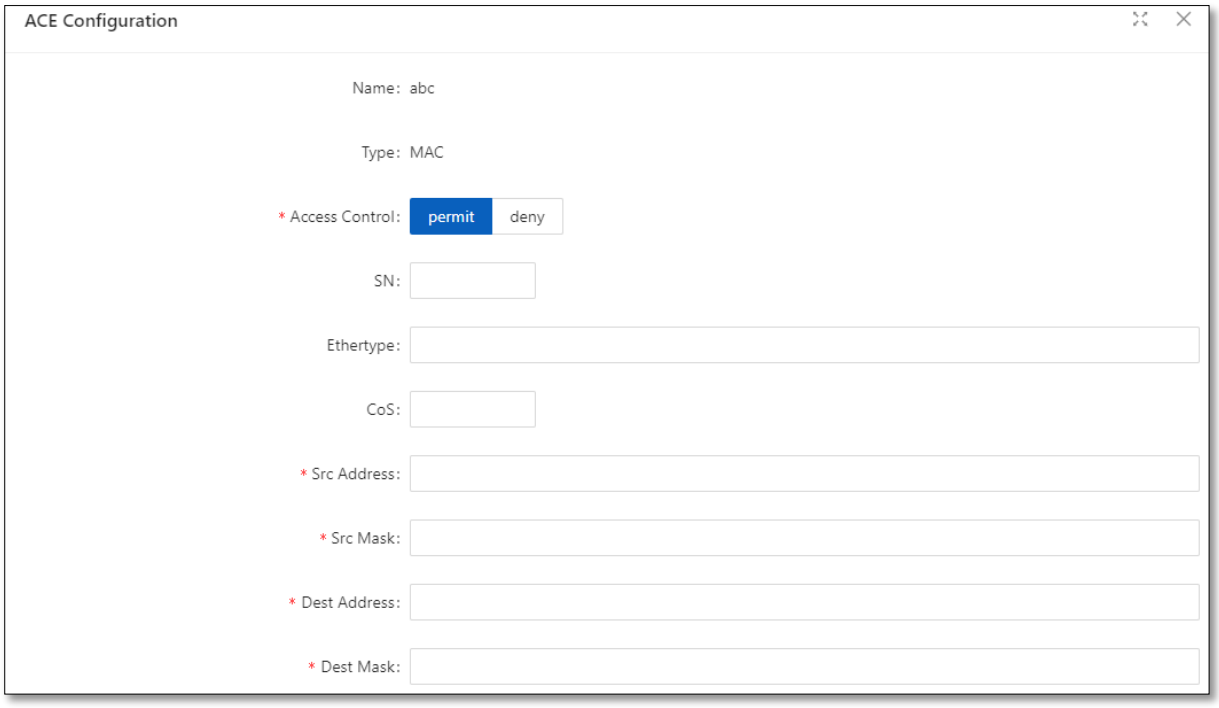


그림 4- 30 포트에 ACL 규칙 적용

메뉴		설명
Access Control	permit	이 규칙과 일치하는 패킷을 해제합니다.
	deny	이 규칙과 일치하는 패킷을 삭제합니다.
SN		규칙 메뉴 순서 번호
Ethertype		이더넷 프로토콜 유형, 범위(0x05DD-0xFFFF)
CoS		메시지의 Cos 값, 범위(0-7)
Src Address		소스 MAC 주소(예: 00.d0.f 8.22.33.40)
Src Mask		소스 MAC 주소(예: 00.d0.f 8.22.33.40) MAC 주소 마스크가 반전됩니다. MAC 주소의 처음 24 자리와 일치하면 마스크는 ffff.ff00.0000 입니다. 여기서는 0000.00ff.ffff 로 구성해야 합니다.
Dest Address		대상 MAC 주소(예: 00.d0.f 8.22.33.41)
Dest Mask		대상의 MASK

표 4- 19 MAC ACL 에 대한 설명

5. ACE 를 구성하고 확인을 클릭합니다.

6. "Port Configuration"아래의 Batch Edit 을 클릭하여 ACL 포트 구성 페이지로 들어가서 해당 포트의 ACL 규칙을 선택한 후 확인을 클릭합니다.

4.7 QoS

4.7.1 개요

서비스 품질(QoS)은 고객 요구를 충족하는 네트워크의 능력을 반영합니다. 인터넷에서 QoS 는 네트워크가 다양한 서비스의 패킷을 전달하는 능력을 평가합니다. 네트워크는 다양한 서비스를 제공할 수 있으므로 평가는 다양한 기준에 기초할 수 있습니다. 일반적으로 QoS 성능은 패킷 전달 과정에서 대역폭, 지연, 패킷 손실률을 기준으로 측정됩니다.

4.7.2 QoS 설정

- QoS 활성화

1. Advance > Security > Qos Configuration 메뉴에서 QoS Global Configuration 페이지로 접속합니다.

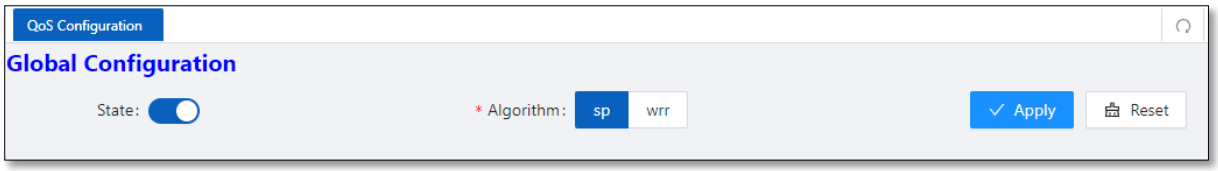


그림 4- 31 QoS Global 설정

2. State 버튼을 클릭하고 알고리즘을 선택한 후 적용을 클릭하여 Qos 를 활성화합니다.

메뉴	설명		
Qos Configuration	State		Qos Configuration
	Algorithm	Sp	절대 우선순위 스케줄링, 대기열 ID 가 크고 우선순위가 높으며 우선순위가 높은 대기열이 처리된 후에 낮은 우선순위 대기열이 처리됩니다.
		Wrr	로빈 스케줄링 알고리즘은 가장 큰 큐 ID 부터 가장 작은 큐 ID 까지 큐 가중치에 따라 각 큐를 차례로 스케줄링 합니다.

표 4- 20 QoS 요약 설명

- QoS 매핑

1. 현재 페이지에서 "Qos Mapping" 아래의 Queue 버튼을 클릭하면 그림과 같이 Queue Configuration 페이지로 접속합니다.

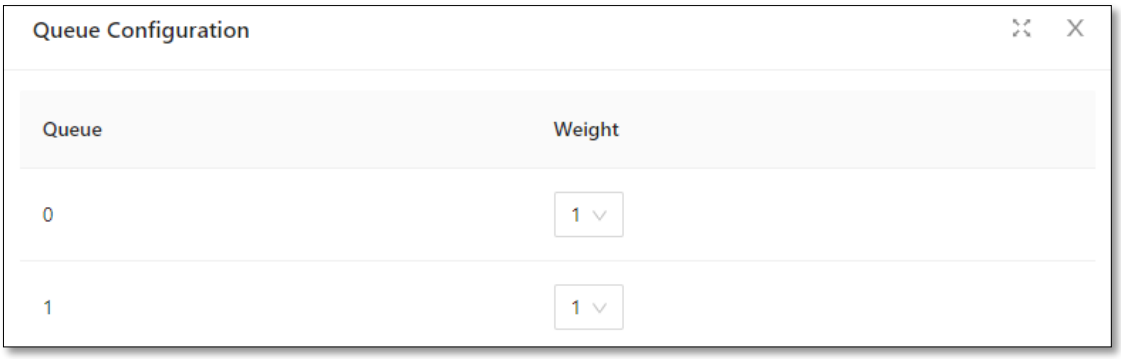


그림 4- 32 QoS 대기열 설정

메뉴	설명	
Queue weight	Queue	<0, 7>
	weight	<0, 32>, 값이 클수록 가중치가 높아지고, 채널 혼잡 상황에서 이 큐에 있는 패킷을 우선적으로 처리할 확률이 높아지며, 0 은 무한대를 의미합니다.

표 4- 21 QoS 설정 설명

2. . "Qos Mapping" 아래의 Cos 버튼을 클릭하여 그림과 같이 Cos 설정 페이지로 접속합니다.

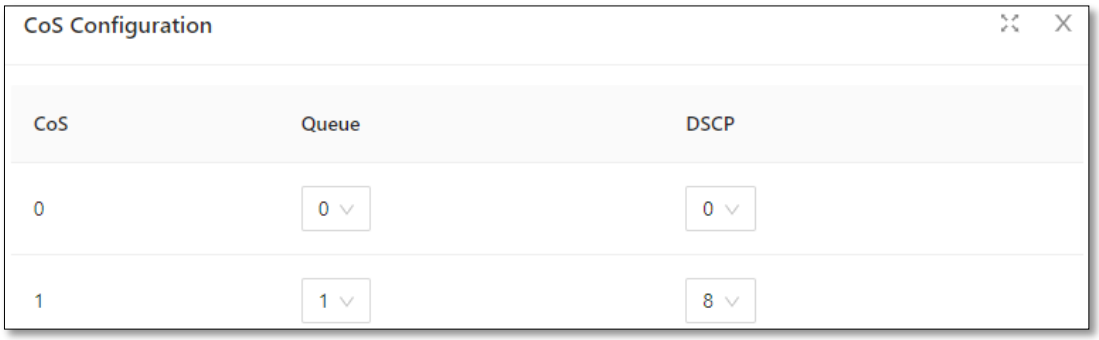


그림 4- 33 QoS CoS 설정

메뉴		설명
CoS Configuration	CoS	<0, 7>
	Queue	< 0, 7>, Cos - 포트에 표시된 cos 를 기반으로 하는 큐 매핑 관계, 패킷 송신 큐 수정은 포트가 신뢰 없음, 신뢰 cos 또는 신뢰 dscp 및 비 ip 패킷으로 설정된 경우 적용됩니다.
	DSCP	cos-dscp 매핑 관계는 포트가 신뢰 없음, 신뢰 cos 또는 신뢰 dscp 로 설정되고 IP 패킷이 아닌 경우 적용됩니다. 패킷 dscp 값을 수정합니다.

표 4- 22 CoS 설정 설명

3. "Qos Mapping" 아래의 DSCP 버튼을 클릭하여 다음과 같이 DSCP 설정 페이지로 접속합니다.

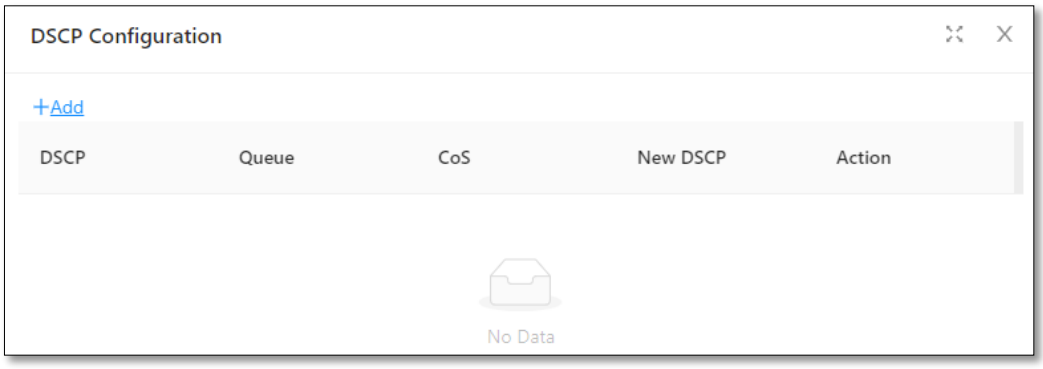


그림 4- 34 QoS DSCP 설정

메뉴		설명
DSCP Map	DSCP	<0, 63>
	Queue	< 0, 7>, 포트가 트러스트 dscp 및 ip 패킷으로 설정될 때 적용되는 dsp-queue 매핑 관계, 패킷 내보내기 큐 수정
	CoS	< 0, 7>, 포트가 트러스트 dscp 및 ip 패킷으로 설정될 때 적용되는 dscp-cos 매핑 관계, 패킷의 cos 필드를 수정합니다.
	Nes DSCP	< 0, 63 >, 포트가 트러스트 dscp 및 ip 패킷으로 설정될 때 적용되는 dscp-dscp 매핑 관계는 먼저 dscp-dscp 매핑을 수행한 다음 dscp-cos 매핑을 수행합니다.

표 4- 23 CoS 설정 설명

- 클래스 설정

1. 현재 페이지에서 "Class 설정" 아래 +Add 버튼을 클릭하면 그림같이 Class 설정 페이지로 진입합니다.

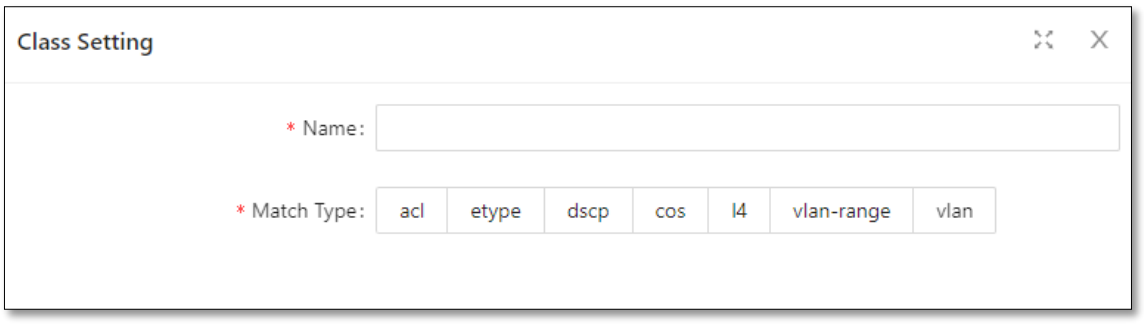


그림 4- 35 클래스 설정 페이지

메뉴		설명
Class Setting	Name	카테고리 생성, 카테고리 이름 정의
	Match	일치 유형을 정의하고 관련 ACL 을 지원합니다. 패킷 etype, dscp, cos, l4port, vlan 필드 일치 지원

표 4- 24 클래스 설정 설명

- 정책 설정

1. 현재 페이지에서 "Policy Setting" 아래의 +Add 정책 추가 버튼을 클릭하여 그림과 같이 정책 설정 페이지로 접속합니다.



그림 4- 36 클래스 정책 설정

2. " Policy Setting " 아래의 +ADD 정책 규칙 추가 버튼을 클릭하여 정책 규칙 설정 페이지로 접속합니다.

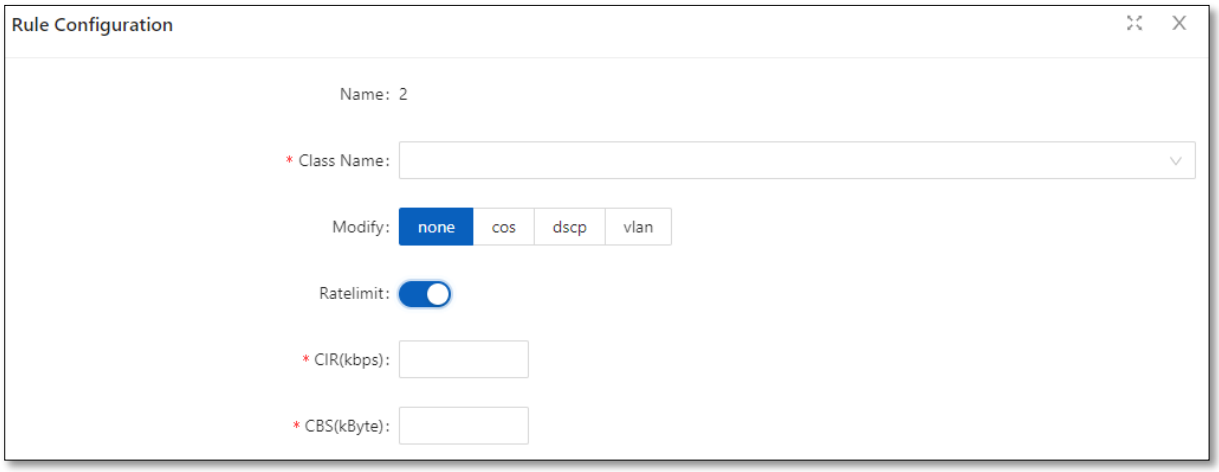


그림 4- 37 규칙 설정 페이지

메뉴		설명
Rule Configuration	Name	규칙 이름
	Class Name	정책 생성, 정책 이름 정의
	Modify	정책은 cos, dscp, vlan 및 기타 작업 수정을 지원합니다.
	Ratelimit	전략에 대응하는 액션 2, 속도 제한
	CIR	속도 제한, 단위 kbps
	CBS	버스트 용량, 단위 Kbyte

표 4- 25 클래스 설정 설명

- 포트 설정

1. 현재 페이지에서 "Port Configuration" 아래의 +일괄 편집 버튼을 클릭하여 설정 페이지로 접속합니다.

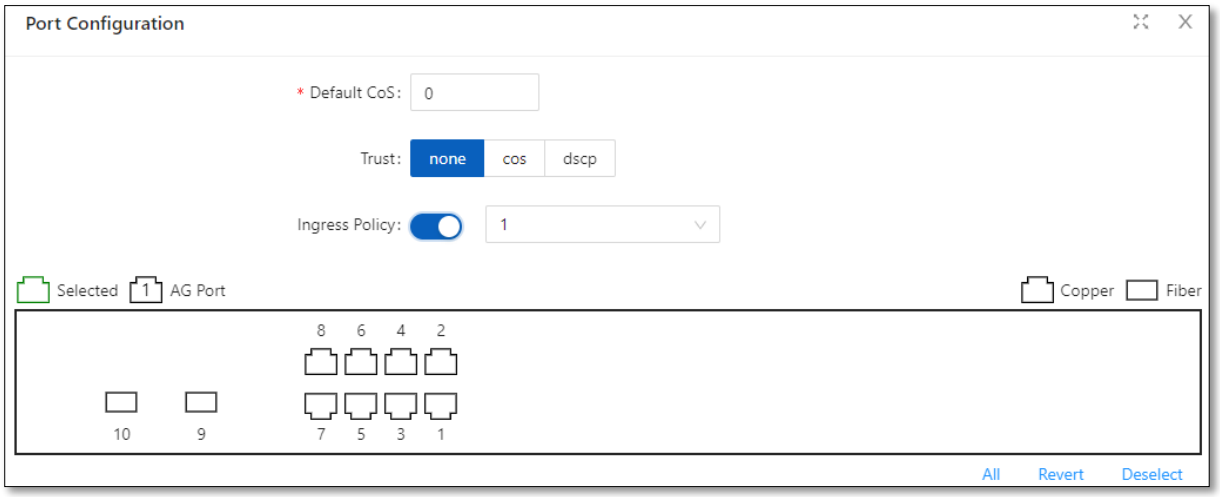


그림 4- 38 포트 설정

메뉴		설명
Port Configuration	Default CoS	< 0, 7>, 설정 포트를 신뢰할 수 없거나 설정을 신뢰할 수 있지만 메시지가 신뢰 조건을 충족하지 않는 경우 포트 기본 cos 를 사용하여 수신 메시지를 표시합니다.
	Trust	cos, 신뢰 dscp 설정을 지원합니다. 신뢰 없음 모드에 있는 경우 시작 단계에서는 포트의 기본 cos 에 따라 메시지의 cos 필드와 dscp 필드를 수정합니다. 신뢰 cos 가 설정되면 태그가 지정되지 않은 메시지에 대한 신뢰 없음 모드와 동일하고 태그가 지정된 메시지에 대해 자체 cos 가 있는 메시지를 선택합니다. trust dscp 설정 시 ip 패킷의 경우 dscp 가

		포함된 패킷을 선택하고, non-ip 패킷의 경우 trust cos 모드와 동일합니다.
	Ingress Policy	수신 정책 선택

표 4- 26 포트 설정 설명

4.8 Dos

4.8.1 개요

서비스 거부(DoS) 공격은 컴퓨터나 네트워크가 정상적인 서비스를 제공하지 못하도록 하는 것을 목표로 합니다. DoS 공격에는 여러 종류가 있으며 구현 방법도 다양합니다. 공통적인 특징은 피해자 호스트나 네트워크가 제때 외부 요청을 수신하고 처리할 수 없다는 것입니다. 다음은 일반적인 DoS 공격 유형입니다.

- SYN 플러드 메시지 공격: SYN 플러드 공격은 현재 네트워크에서 가장 흔한 DDOS 공격이지만 가장 고전적인 DoS 공격이기도 합니다. 가짜 소스 주소가 있는 많은 수의 공격 메시지를 네트워크 서비스 포트로 보내면 대상 서버 연결 대기열이 가득 차서 다른 합법적인 사용자의 액세스가 차단됩니다.
- ICMP 플러드 메시지 공격: ICMP Flood 공격은 짧은 시간 내에 대상 호스트에 대량의 ping 패킷을 보내 호스트 리소스를 소모하는 DDOS 공격입니다. 호스트는 리소스가 고갈되면 다른 서비스를 제공할 수 없습니다.
- ARP 플러드 메시지 공격: ARP 플러드 공격은 짧은 시간 내에 대상 호스트에 많은 수의 ARP 요청 패킷을 보내고 호스트 리소스를 소모하는 DDOS 공격입니다. 호스트 리소스가 고갈된 후에는 다른 ARP 요청에 응답할 수 없습니다.
- NULL SCAN 메시지 공격: NULL SCAN 공격은 주로 공격자가 대상 호스트의 IP 에 플래그 없이 TCP 패킷을 보내고 운영 체제의 일부가 RST 메시지를 적극적으로 피드백하여 공격자가 세션을 닫지 않는 포트를 얻는 것입니다. NULL SCAN 방지 공격은 TCP 플래그 비트가 없는 TCP 메시지를 삭제하여 공격자가 NULL SCAN 을 통해 각 포트의 닫힘을 얻은 후 후속 공격을 시작하는 것을 효과적으로 방지할 수 있습니다.
- SYN 및 FIN 이 있는 TCP 메시지: 일반적으로 SYN 부호(연결 요청 부호)와 FIN 부호(연결 제거 부호)는 하나의 TCP 메시지에 나타날 수 없으며 RFC 는 IP 스택이 이러한 변형된 메시지를 어떻게 처리할지 지정하지 않습니다. 공격자는 이 기능을 이용하여 SYN 및 FIN 설정이 있는 TCP 메시지를 보내 운영 체제 유형을 확인할 수 있습니다.
- ACK 가 없는 FIN 이 있는 TCP 메시지: 일반적인 상황에서 첫 번째 메시지(SYN 메시지)를 제외한 모든 메시지에는 ACK 기호가 있으며, TCP 연결 제거 메시지(FIN 기호가 설정된 메시지)도 포함됩니다. 그러나 일부 공격자는 FIN 이 있고 ACK 가 없는 TCP 메시지를 대상 호스트로 보내 대상 호스트가 충돌할 수 있습니다.
- SYN 및 0-1023 사이의 소스 포트 번호가 있는 TCP 메시지: 0-1023 은 IANA 에서 지정한 알려진 포트 번호이며 대부분 시스템에서 시스템(또는 루트) 프로세스나 권한이 있는 사용자가 실행하는 프로시저에서만 사용할 수 있습니다. 이러한 포트(0-1023)는 첫 번째 TCP

메시지의 소스 포트 번호로 사용할 수 없습니다(SYN 기호가 이미 설정됨). 불법 TCP 메시지 공격 방지 기능을 시작하면 장치는 비 TCP 메시지의 특성에 따라 검사하여 불법이면 삭제합니다.

4.8.2 DoS 설정

Advance > Security > DoS Configuration 을 선택하고 DoS 구성 페이지로 들어갑니다. 이 페이지에는 글로벌 구성, SYN 구성, ICMP 구성, ARP 구성의 네 가지 부분이 있습니다.

- 글로벌 설정

DoS 글로벌 구성 페이지는 그림 4-39 에 나와 있으며, 여기에는 여러 글로벌 안티-DoS 공격 구성이 포함되어 있으며, 구체적인 매개변수는 표 4-27 에 나와 있습니다. 글로벌 SYN 플러드, ICMP 플러드 및 ARP 플러드는 같은 방식으로 구성합니다. 예를 들어 ARP 플러드 구성을 살펴보면 설정 페이지는 그림 4-41 과 같습니다.

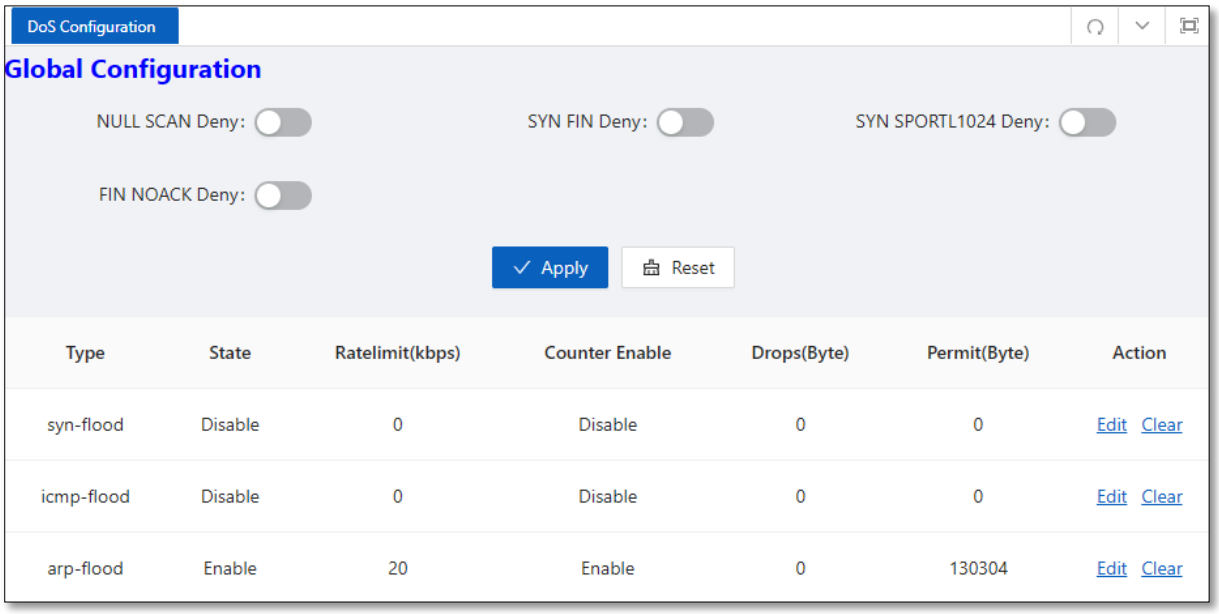


그림 4- 39 글로벌 설정 화면

메뉴	설명
NULL SCAN Deny	전역적 안티-NULL SCAN 공격을 구성하고, 플래그 없이 TCP 메시지를 삭제합니다.
SYN FIN Deny	전역적 안티-SYN FIN 공격을 구성하고, SYN 및 FIN 플래그로 설정된 TCP 메시지를 삭제합니다.
SYN SPORT1024 Deny	글로벌 anti-SYN SPORTL1024 공격을 구성하고 소스 포트(0-1023) TCP 의 동기 메시지를 오픈 후 삭제합니다.

FIN NOACK Deny	전역적 안티-FIN NOACK 공격을 구성하고, ACK 가 설정되지 않은 FIN 이 설정된 TCP 메시지를 삭제합니다.
SYN/ICMP/ARP Flood	터미널이 위치한 Layer 3 인터페이스의 이름
SYN/ICMP/ARP Flood rate-limit	SYN/ICMP/ARP Flood 공격의 속도 제한 범위를 구성하고 값이 0 인 경우 모든 공격 메시지를 거부합니다.
Counter enable	SYN/ICMP/ARP Flood 공격의 카운터 활성화 기능을 구성하고 활성화된 경우 히트 공격 메시지를 계산합니다.

표 4- 27



그림 4- 40 ARP 설정

- 설정

1. Advance > Security > DoS Configuration 선택하여 DoS 구성 페이지로 들어갑니다.
2. 글로벌 구성 테이블에서 편집 버튼을 클릭하여 DoS 공격 방지 생성 으로 들어가고 요구 사항에 따라 설정 값을 채웁니다. 예를 들어 그림 4-41 에 표시된 것처럼 글로벌 ARP 플러드 구성을 사용하고 확인 버튼을 클릭하여 구성을 완료합니다.

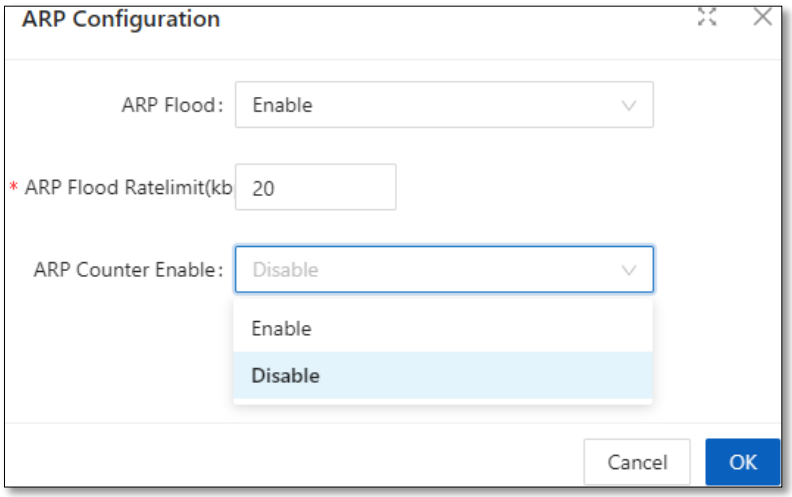


그림 4- 41 ARP flood 설정

3. 위의 단계를 거친 후, 성공적인 DoS 글로벌 구성 페이지를 그림 4-43 처럼 확인 할 수 있습니다.

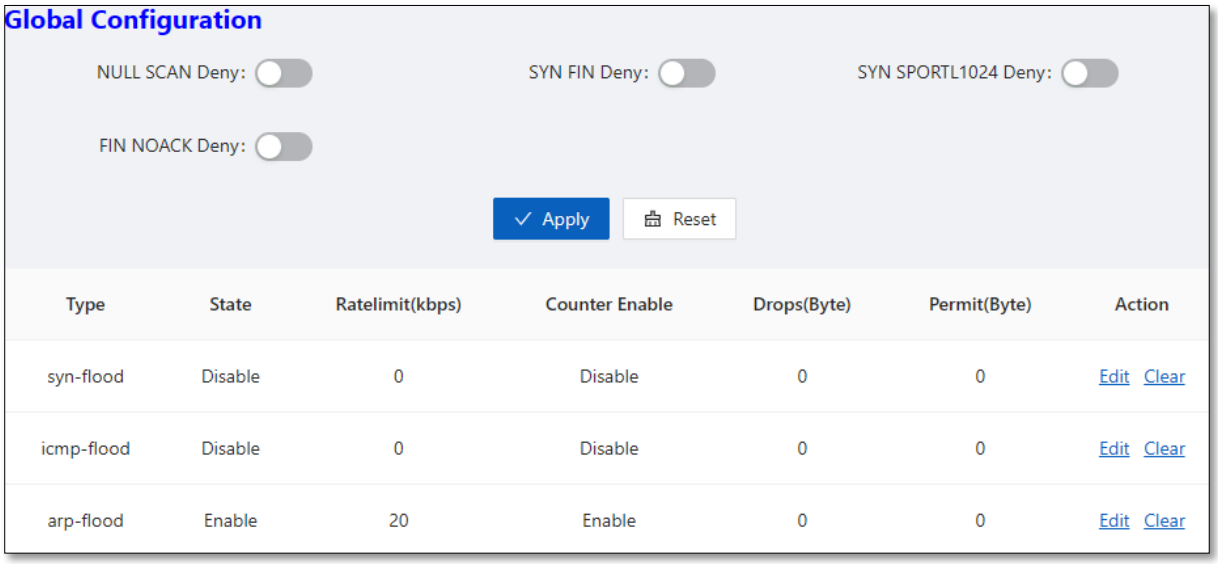


그림 4- 42 Global 설정

- SYN/ICMP/ARP 설정

DoS 공격에 대한 포트 설정에는 SYN Flood, ICMP Flood 및 ARP Flood 가 포함됩니다. 설정 페이지는 그림 4-43~46 에 표시되어 있으며 설정 값 설명은 표 4-28 에 표시되어 있습니다.

메뉴	설명
SYN Flood	SYN Flood attack 활성화
SYN Flood rate-limit	SYN 메시지 attack 흐름 속도 제한.
ICMP Flood	ICMP Flood attack 활성화.
ICMP Flood rate-limit	ICMP 메시지 attack 흐름 속도 제한
ARP Flood	ARP Flood attack 활성화
ARP Flood rate-limit	SYN/ICMP/ARP Flood 공격의 속도 제한 범위를 구성하고 값이 0 인 경우 모든 공격메시지를 거부합니다.
SYN Flood	ARP 메시지 attack 흐름 속도 제한

표 4- 28 SYN/ICMP/ARP 설정

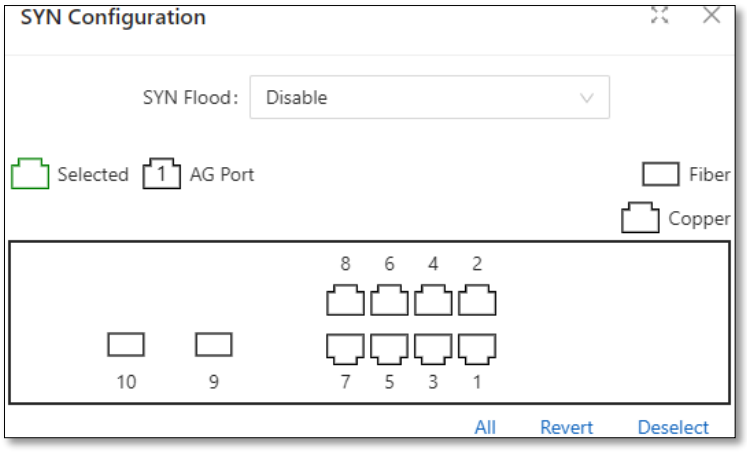


그림 4- 43 SYN 설정 화면

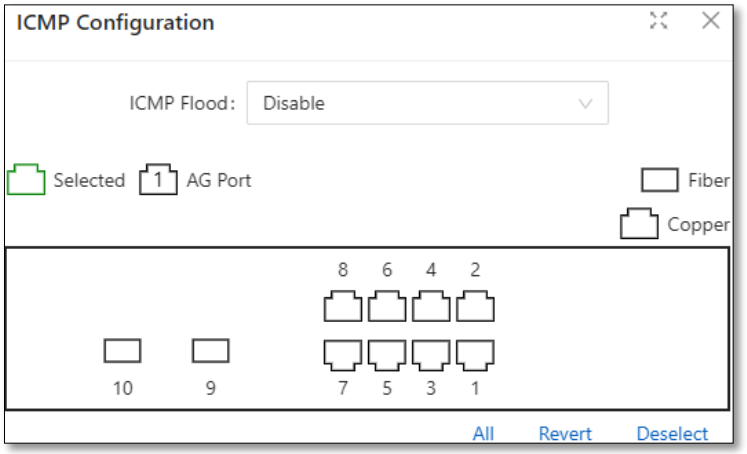


그림 4- 44 ICMP 설정 화면

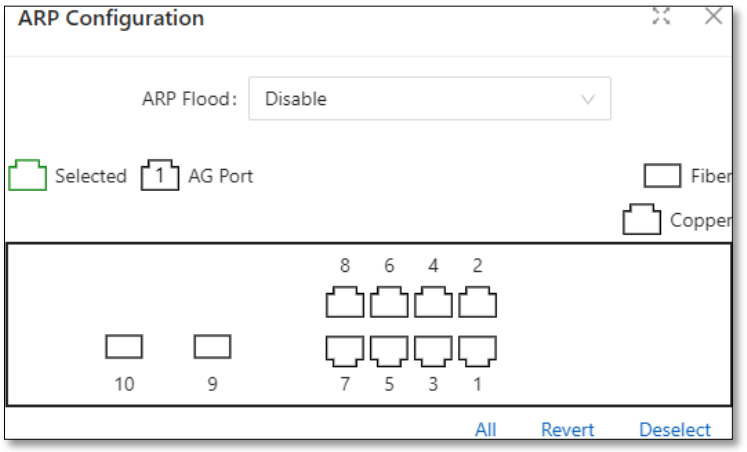


그림 4- 45 ARP 설정 화면

- 설정

1. Advance > Security > DoS Configuration 을 선택하여 DoS 구성 페이지로 들어갑니다.

2. SYN/ICMP/ARP 구성에서 일괄 편집 버튼을 클릭하여 생성 페이지로 들어갑니다. 그림 4-46 과 같이 ARP 구성을 예로 들어보겠습니다.

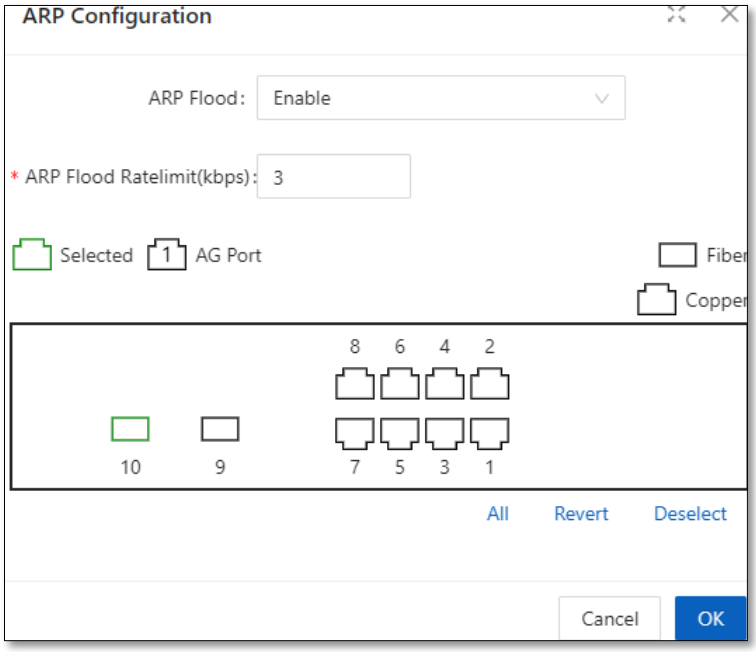


그림 4- 46 ARP 설정

위의 단계를 거치면 성공적인 ARP 설정 페이지가 그림 4-47 에 표시됩니다.

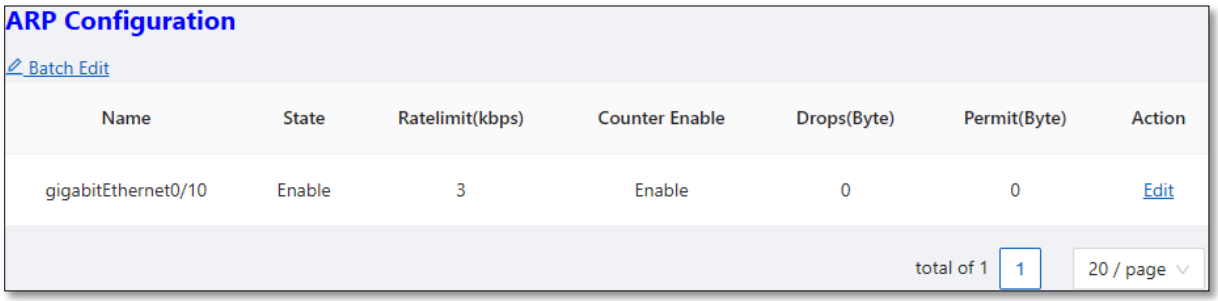


그림 4- 47 ARP 설정 테이블

- 설정 예시

예를 들어 ARP Flood Configuration 을 살펴보면, 다음 네트워킹 요구 사항이 그림 4-49 에 나와 있습니다.

1. 포트 gi0/1 은 FTP 서버에 연결되고 포트 gi0/2 와 gi0/3 은 각각 터미널 장치에 연결됩니다.
2. 포트 gi0/2 의 연결 터미널은 많은 수의 IP 및 MAC 주소를 위조하여 ARP 공격을 시작하므로 FTP 서버는 정상적인 요청 ARP 메시지를 처리할 수 없습니다.

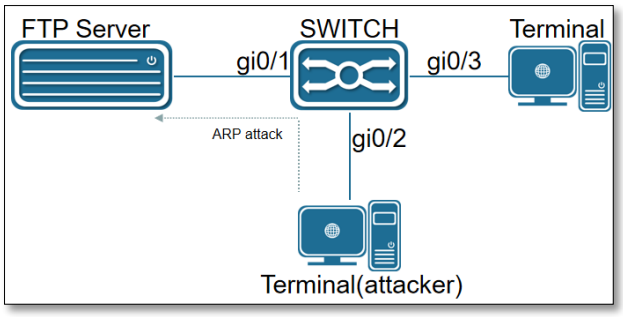


그림 4- 48 설정 예시 구성

3. Advance > Security > DoS Configuration 을 선택하여 DoS 구성 페이지로 들어갑니다.

4. ARP 구성 아래의 일괄 편집 버튼을 클릭하여 ARP 설저으로 들어가고, 포트 패널에서 GigabitEthernet0/2 를 선택하고 확인을 클릭하여 구성을 완료합니다.

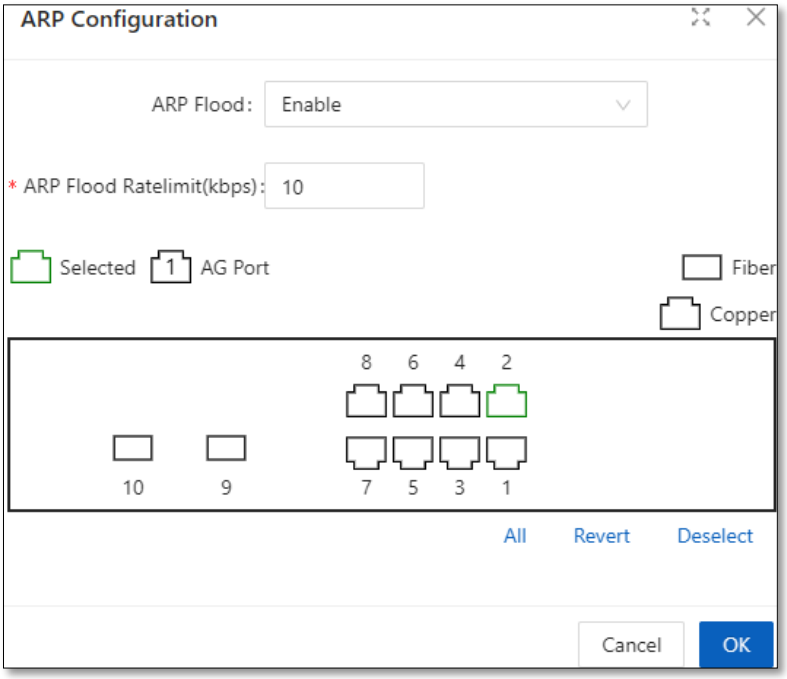


그림 4- 49 ARP 설정 화면

5. 해당 설정을 저장하려면 탐색 모음에서 저장 버튼을 클릭하세요.

4.9 Route

4.9.1 ARP

4.9.1.1 개요

RP 는 IP 주소를 이더넷 MAC 주소와 같은 물리적 주소로 확인합니다. 이더넷 LAN 에서 장치는 ARP 를 사용하여 패킷에 대한 대상 장치의 MAC 주소를 얻습니다.

- ARP 테이블

대상 호스트의 MAC 주소를 얻은 후 장치는 IP-MAC 매핑을 자체 ARP 테이블에 넣습니다. 이 매핑은 향후 동일한 대상으로 패킷을 전달하는 데 사용됩니다.

ARP 테이블은 동적 및 정적 ARP 메뉴를 저장합니다.

- 동적 ARP 메뉴

ARP 는 동적 메뉴를 자동으로 생성하고 업데이트합니다. 동적 ARP 메뉴는 해당 에이징 타이머가 만료되거나 출력 인터페이스가 다운되면 제거되며 정적 ARP 메뉴로 덮어쓸 수 있습니다.

- 정적 ARP 메뉴

정적 ARP 메뉴는 수동으로 설정 및 유지 관리됩니다. 동적 ARP 메뉴로 인해 오래되거나 덮어쓰일 수 없습니다.

정적 ARP 메뉴는 공격 패킷이 정적 ARP 메뉴의 IP-MAC 매핑을 수정할 수 없기 때문에 장치 간 통신을 보호합니다.

4.9.1.2 Static ARP 설정

- Static ARP

1. Monitor > ARP Information 메뉴에서 Static ARP displaying 페이지로 접속합니다.



그림 4- 50 ARP Information 페이지

메뉴	설명
IP Address	터미널 IP 주소
MAC address	단말기맥주소
Interface	터미널이 위치한 Layer 3 인터페이스의 이름
Type	ARP 주소 유형

표 4- 29 Static ARP 설명

- Static ARP 설정

1. Advance > Layer3 > Static ARP 메뉴에서 Static ARP configration 페이지로 접속합니다.
2. +ADD 버튼을 클릭하여 설정페이지로 접속합니다.
3. IP 주소 및 MAC 주소를 설정합니다.
4. OK 버튼을 클릭하여 설정을 완료합니다.

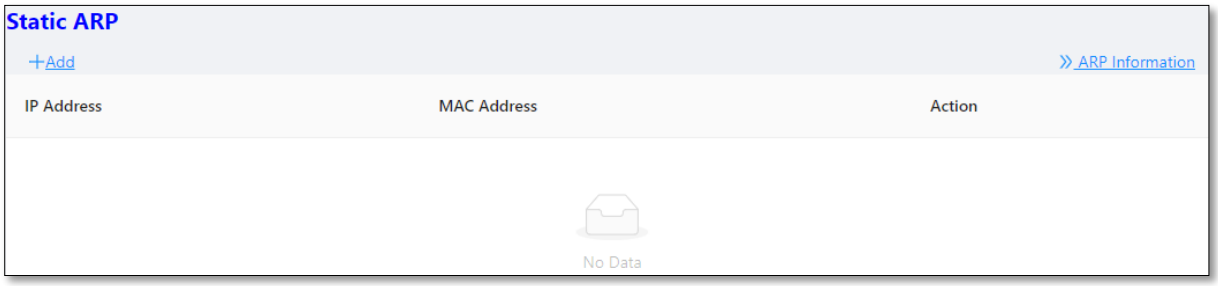


그림 4- 51 Static ARP 설정



그림 4- 52 새로운 Static ARP 생성

4.9.2 Route

라우터는 인터넷에서 패킷 라우팅을 담당합니다. 라우터는 다음을 선택합니다. 수신된 패킷의 목적지 주소에 따른 적절한 경로와 패킷을 다음 라우터로 전달합니다. 경로의 마지막 라우터는 패킷을 대상 호스트로 보냅니다.

4.9.2.1 라우팅 테이블

라우터는 라우팅 테이블을 통해 패킷을 전달합니다. 테이블의 각 메뉴는 다음을 지정합니다. 물리적 인터페이스에서 패킷은 다음 홉(다음 라우터)에 도달하기 위해 나가야 합니다. 직접 연결된 목적지. 라우팅 테이블의 경로는 출발지에 따라 세 가지 범주로 분류됩니다.

- Direct routes : 인터페이스라고도 알려진 데이터 링크 프로토콜에 의해 발견된 경로
- Static routes : 수동으로 설정된 경로입니다.
- Dynamic routes : 라우팅 프로토콜에 의해 동적으로 검색되는 경로입니다.
- Destination IP address : 대상 IP 주소 또는 대상 네트워크입니다.
- Mask (IPv4)/prefix length (IPv6) : 대상의 주소와 함께 네트워크 주소를 지정합니다.
- Outbound interface: Specifies the interface through which a matching IP packet is to be forwarded.
- Next hop : 경로의 다음 홉 라우터 주소를 지정합니다.
- Preference for the route : 동일한 목적지로 가는 경로는 다양한 방법으로 찾을 수 있습니다. 라우팅 프로토콜 또는 수동으로 설정, 라우팅 프로토콜 및 정적 경로 우선순위가 다르게 설정되어 있습니다. 우선순위가 가장 높은 경로(가장 작은 경로) 값)이 최적의 경로로 선택됩니다.

4.9.2.2 Static Route

static route 는 수동으로 구성됩니다. 네트워크의 토폴로지가 단순한 경우 네트워크가 정상적으로 작동하려면 static route 만 구성하면 됩니다. static route 를 적절하게 설정하고 사용하면 네트워크 성능이 향상되고 중요한 네트워크 애플리케이션에 대한 대역폭이 보장될 수 있습니다.

static route 사용의 단점은 네트워크 토폴로지 변경 사항에 적응할 수 없다는 것입니다. 네트워크에 결함이나 토폴로지 변경이 발생하면 일부 경로에 연결할 수 없습니다. 이 경우 네트워크 관리자는 고정 경로를 수동으로 수정해야 합니다.

static route 를 구성하는 동안 필요에 따라 출력 인터페이스 또는 다음 홉 주소를 지정할 수 있습니다. 다음 홉 주소는 로컬 인터페이스의 IP 주소일 수 없습니다. 그렇지 않으면 경로 설정이 적용되지 않습니다.

실제로 라우터는 해당 링크 계층 주소를 확인하기 위해 일치하는 메뉴의 다음 홉 주소를 사용해야 하기 때문에 모든 경로 메뉴에 대해 다음 홉 주소를 식별해야 합니다.

4.9.2.3 static route 설정

- Static Route

1. Advance > Layer3 > Static Route 메뉴에서 Static Route 페이지로 접속합니다.

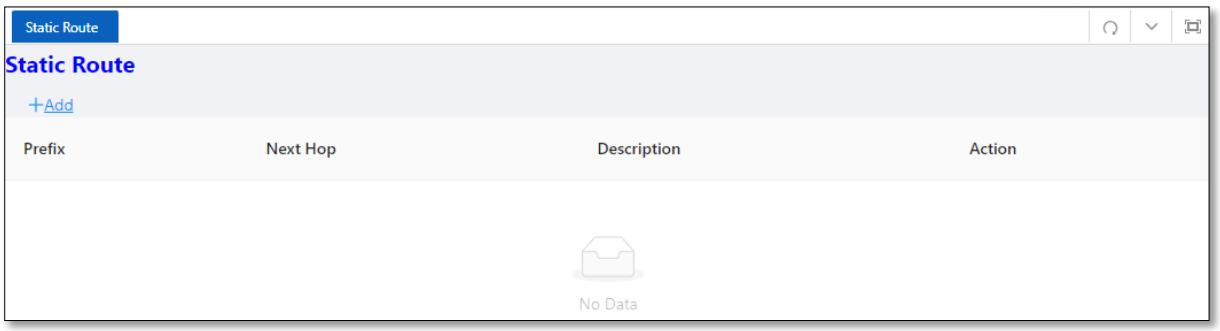


그림 4- 53 Static Route

메뉴	설명
Prefix	라우팅 접두사 주소 또는 라우팅 네트워크 세그먼트 예를 들어 공통 경로 0.0.0.0/0 192.168.1.1, 접두사 IP 는 0.0.0.0 입니다.
Next Hop	다음 홉 IP 주소 노선
Description	경로 설명 정보, 선택적 설정
Action	삭제 또는 수정

표 4- 30 Static Route 설명

- Static Route 생성

1. Configuration > VLAN 메뉴에서 VLAN ID 를 생성합니다.

2. Configuration > Port > Port Configuration > L3 메뉴에서 포트를 생성합니다.

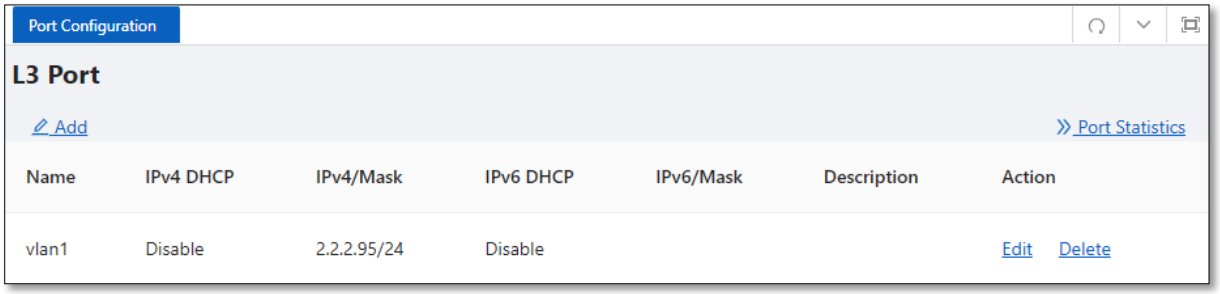


그림 4- 54 L3 Port 생성

3. Advance > Layer3 > Static Route 메뉴에서 페이지에 접속한 후 +ADD 버튼을 클릭하여 Crating 페이지로 접속합니다.

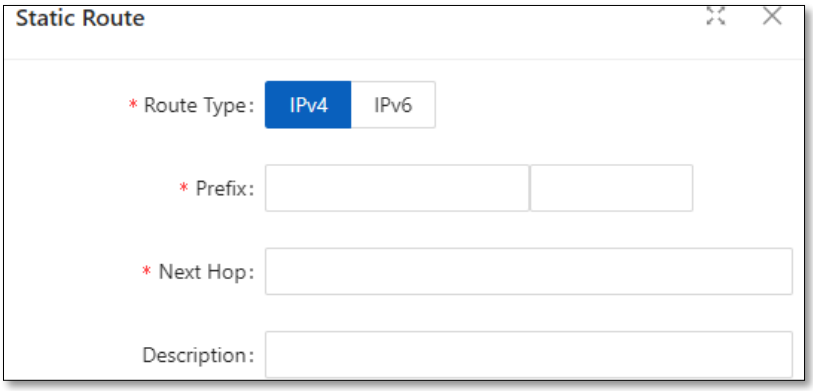


그림 4- 55 Static Route 생성

NOTE:

- 새 SVI 포트를 추가하면 기본 관리 IP 주소가 자동으로 삭제됩니다. 새 SVI 포트에 계속 액세스할 수 있는지 확인하십시오.

5. Maintenance

5.1 System 설정

시스템 설정은 호스트 이름 설정, Telnet 서비스, SSH, HTTP, HTTPS 및 관리 IP 설정을 제공합니다.

5.1.1 Host name 설정

1. Maintenance > system configuration 메뉴에서 system configuration 페이지에 접속합니다.



그림 5- 1 Management 정보 페이지

5.1.2 서비스 활성화

서비스 관리 모듈은 FTP, Telnet, SSH, SFTP, HTTP 및 HTTPS 와 같은 유형의 서비스를 제공합니다. 필요에 따라 서비스를 활성화하거나 비활성화할 수 있습니다. 이를 통해 시스템의 성능과 보안을 강화할 수 있어 장치를 안전하게 관리할 수 있습니다.

- Telnet Server

Telnet 프로토콜은 네트워크에서 원격 로그인 및 가상 터미널 기능을 제공하는 응용 프로그램 계층 프로토콜입니다.

- SSH Server

SSH(Secure Shell)는 원격 장치에 안전하게 로그인하는 접근 방식을 제공합니다. 암호화 및 강력한 인증을 통해 IP 스푸핑, 일반 텍스트 비밀번호 가로채기 등의 공격으로부터 장치를 보호합니다.

- HTTP 서버

HTTP(Hypertext Transfer Protocol)는 인터넷을 통해 웹 페이지 정보를 전송하는 데 사용됩니다. 이는 TCP/IP 프로토콜 제품군의 애플리케이션 계층 프로토콜입니다. HTTP 서비스가 활성화된 HTTP 프로토콜을 사용하여 장치에 로그인하고 웹 기반 네트워크 관리를 통해 장치에 액세스하고 제어할 수 있습니다.

- HTTPS 서버

보안 HTTP(HTTPS)는 SSL(Security Socket Layer) 프로토콜을 지원하는 HTTP 프로토콜을 나타냅니다. HTTPS 의 SSL 프로토콜은 다음과 같은 방법으로 장치의 보안을 강화합니다.

  - SSL 프로토콜을 사용하여 합법적인 클라이언트가 장치에 안전하게 액세스할 수 있도록 보장하고 불법 클라이언트를 금지합니다.
  - 데이터 보안과 무결성을 보장하기 위해 HTTPS 클라이언트와 장치 간에 교환되는 데이터를 암호화하여 장치의 보안 관리를 실현합니다.
  - 불법 클라이언트의 공격을 더욱 방지하기 위해 클라이언트의 접근 권한을 제어하는 장치에 대한 인증서 속성 기반 접근 제어 정책을 정의합니다.

- 서비스 설정

1. Maintenance > system configuration 메뉴에서 system configuration 페이지로 접속합니다.
2. 서비스 앞의 확인란을 선택하고 적용 버튼을 클릭하여 서비스를 활성화합니다.

3. HTTPS 서버가 활성화되면 인증서와 개인 키를 업로드해야 합니다. 인증서를 지정하지 않으면 장치는 기본 인증서를 사용합니다.

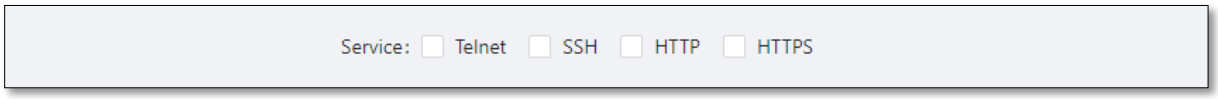


그림 5- 2 서비스 페이지

5.1.3 Management IP

1. Maintenance> system configuration 메뉴에서 system configuration 페이지로 접속합니다.

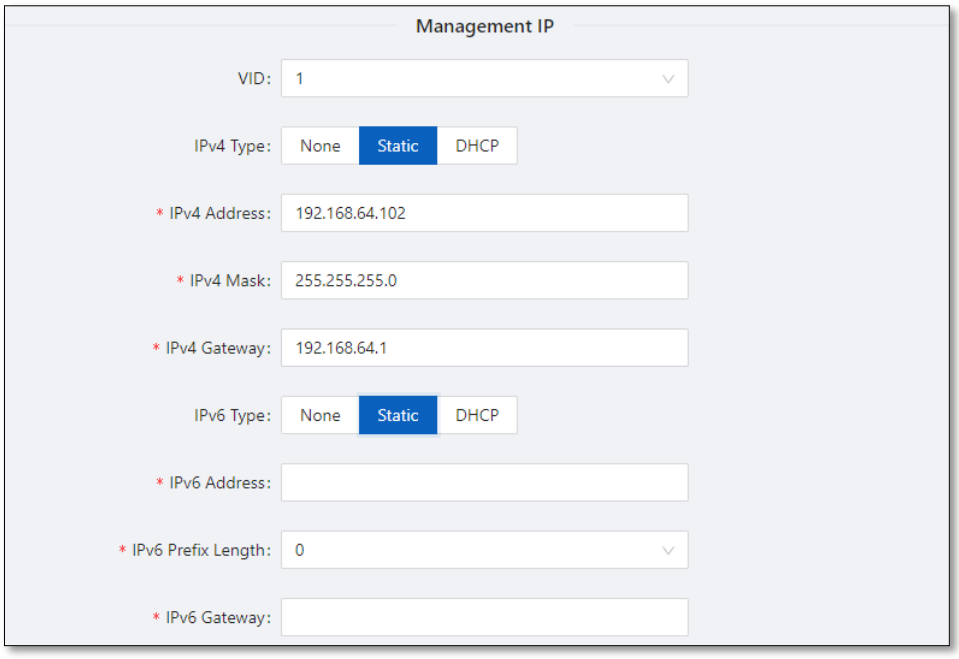


그림 5- 3 Management IP

메뉴	설명
VID	관리 VLAN ID 를 지정합니다. 기본 관리 VLAN 은 1 입니다.
IPv4 Type	None : IPv4 관리 주소는 사용되지 않습니다. Static : IPv4 주소와 마스크 길이를 수동으로 지정하려면 이 옵션을 선택하세요. DHCP : DHCP 를 통해 IPv4 주소를 가져오는 옵션을 선택합니다.
IPv4 Address	IPv4 관리 주소를 지정합니다. 기본 IP 는 192.168.56.166 입니다.
IPv4 Mask	IPv4 관리 마스크를 지정합니다. 기본 마스크는 255.255.255.0 입니다.
IPv4 Gateway	IPv4 관리 게이트웨이를 지정합니다. 기본 게이트웨이는 192.168.56.1 입니다.
IPv6 Type	None : IPv6 관리 주소는 사용되지 않습니다. Static : IPv6 주소와 마스크 길이를 수동으로 지정하려면 이 옵션을 선택하세요. DHCP : DHCP 를 통해 IPv6 주소를 가져오는 옵션을 선택합니다.
IPv6 Address	IPv6 관리 주소를 지정합니다.

IPv6 Prefix Length	IPv6 관리 주소 접두사 길이를 지정합니다.
IPv6 Gateway	IPv6 관리 게이트웨이를 지정합니다.

표 5- 1 Management IP 설정

5.2 File Management

파일 관리 모듈에는 기본 정보, 이미지 관리, 설정 관리, 인증서 관리, 페이지 패키지 관리 기능이 포함되어 있습니다.

5.2.1 Basic Information

1. Maintenance > File Management > Basic Information 메뉴로 접속합니다. 각 파티션별 사용량을 확인 할 수 있으며 Clean 을 클릭하면 시스템 로그가 삭제 됩니다.

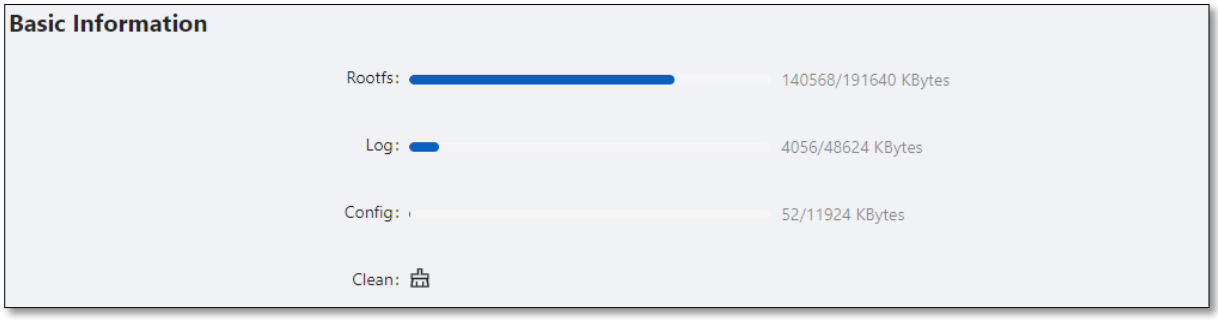


그림 5- 4 Basic information

5.2.2 Image Management

소프트웨어 업그레이드를 사용하면 현재 호스트에서 대상 응용 프로그램 파일을 얻고 해당 파일을 다음 재부팅 시 사용할 기본 부팅 파일 또는 백업 부팅 파일로 설정할 수 있습니다.

NOTE :

- 소프트웨어 업그레이드에는 시간이 걸립니다. 업그레이드 절차 중에는 웹 인터페이스에서 어떤 작업도 수행하지 마십시오. 그렇지 않으면 업그레이드 작업이 중단될 수 있습니다.

1. Maintenance > File Management > Image Management 메뉴로 접속합니다.

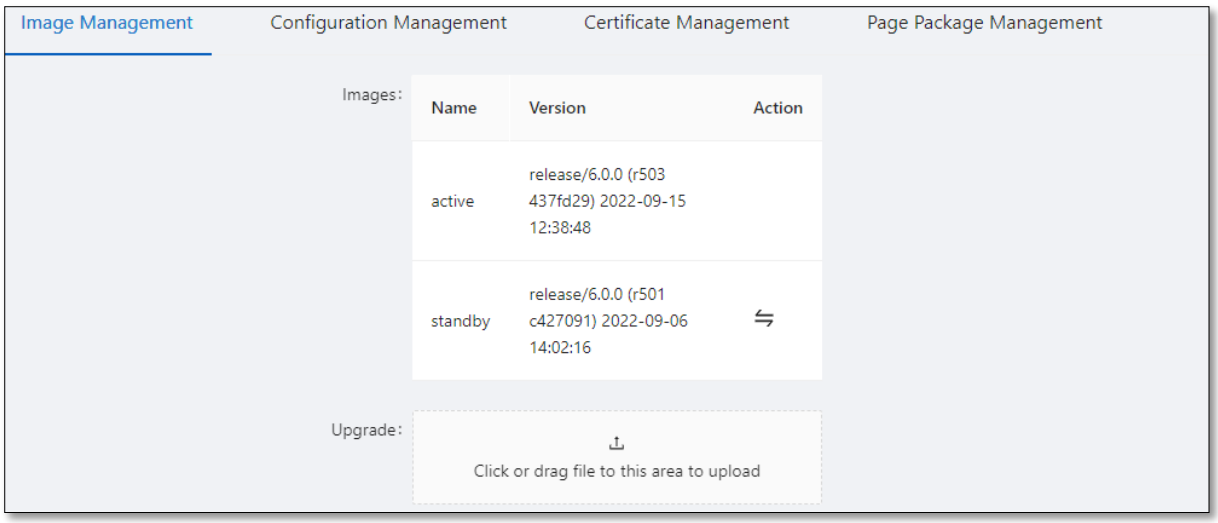


그림 5- 5Image Management 페이지

2. 업그레이드 버튼을 클릭하고 팝업 대화 상자에서 장치에 해당하는 업그레이드 파일을 선택합니다. 업그레이드 파일은 *.bin 형식이며 업그레이드 프로세스는 그림 5-6 에 표시됩니다. 업그레이드가 완료되면 장치가 재부팅 됩니다.

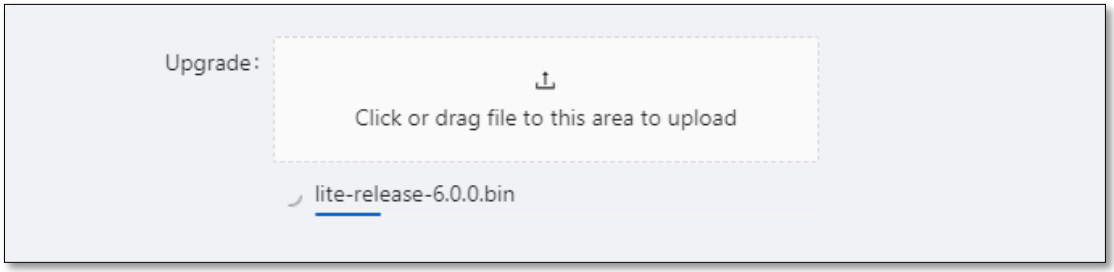


그림 5- 6 firmware image 페이지

5.2.3 Configuration Management

1. Maintenance> File Management> Image Management 메뉴로 접속합니다.

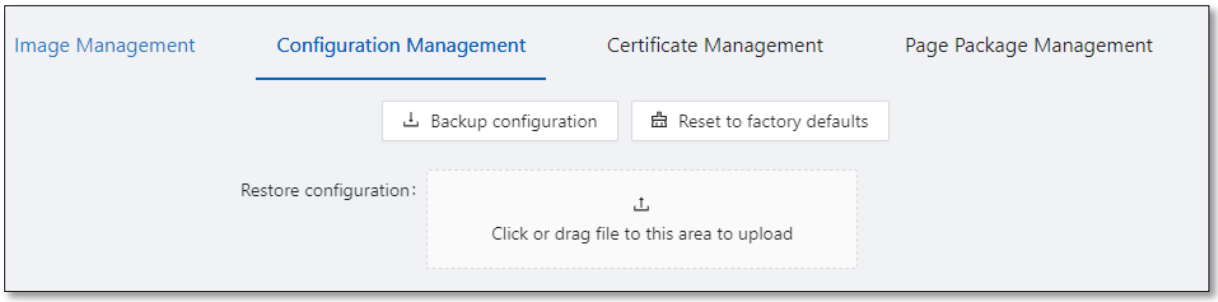


그림 5- 7 File Management 설정

- Backup Configuration

백업 버튼을 클릭하면 파일 다운로드 대화 상자가 나타납니다. 파일을 로컬에 저장할 수 있습니다.

- Restore configuration

이 그림에서 파일 선택 버튼을 클릭하면 파일 업로드 대화 상자가 나타납니다. *를 선택할 수 있습니다. conf 파일을 업로드하면 장치가 재부팅 됩니다.

- Reset to Factory Defaults

이 작업을 수행하면 시스템이 공장 기본값으로 복원되고 현재 설정 파일이 삭제되며 재부팅 됩니다.

5.2.4 Configuration Management

HTTPS 를 활성화하면 그림 5-8 과 같이 인증서와 개인 키를 업로드해야 합니다. 인증서를 지정하지 않으면 장치는 기본 인증서를 사용합니다.

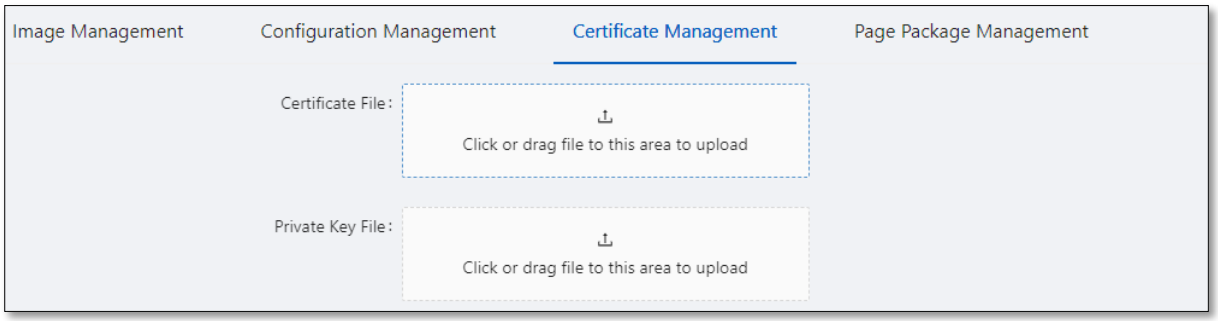


그림 5- 8 Configuration Management

5.2.5 Page Package Management

페이지 패키지 관리 모듈은 그림 5-9 와 같이 로컬 호스트에서 대상 페이지 패키지 파일을 가져와 해당 파일을 장치 페이지 패키지 파일로 적용하는 기능을 제공합니다.

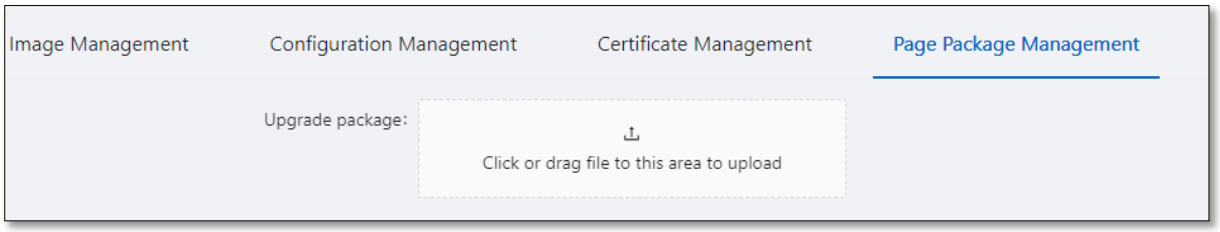


그림 5- 9 Page Package Management

5.3 User Management

User Management 는 아래의 메뉴를 설정할 수 있습니다.

- 사용자 이름, 비밀번호를 설정합니다.
- 새로운 사용자를 만들 수 있습니다.

1. Maintenance> User Management 메뉴에 접속합니다.

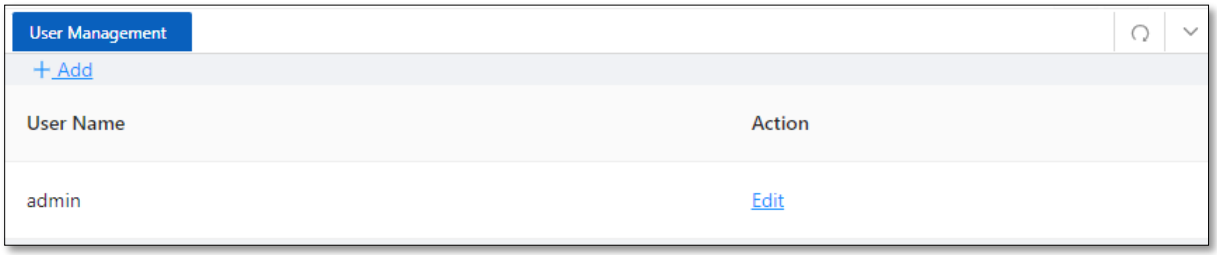


그림 5- 10 User Management

메뉴		설명
Account	Name	사용자 이름
	Edit	비밀번호를 변경하려면 클릭하세요.
	Delete	사용자 계정을 삭제하려면 클릭하세요.
	+Add...	새 사용자를 생성하려면 클릭하세요.

표 5- 2 사용자

5.4 Time Management

Time Management 를 사용하면 웹 인터페이스에서 장치 시스템 시간을 표시하고 설정할 수 있습니다. 장치는 NTP 서버 시간의 수동 설정 및 자동 동기화를 통해 시스템 시간 설정을 지원합니다. 관리자는 각 장치의 시스템 시계를 변경하여 네트워크 내의 모든 장치 간에 시간 동기화를 유지할 수 없습니다. 이는 시간이 많이 걸리는 작업이고 시계 정밀도를 보장할 수 없기 때문입니다. RFC 1305 에 정의된 NTP(Network Time Protocol)는 분산된 시간 서버와 클라이언트 간의 시간 유지를 동기화합니다. NTP 는 전체 네트워크 내에서 빠른 시계 동기화를 가능하게 하며 높은 시계 정밀도를 보장하므로 장치는 일관된 시간을 기반으로 다양한 애플리케이션을 제공할 수 있습니다.

5.4.1 시스템 시간 보기

1. Maintenance> Time Management 메뉴로 접속합니다. 현재 시스템 시간과 시계상태가 표시됩니다.

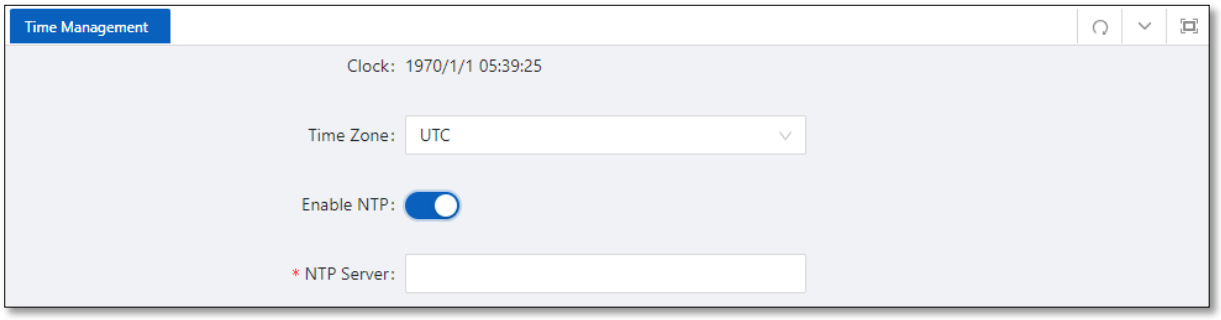


그림 5- 11 시스템 시간 설정

메뉴	설명
Clock	시스템 날짜 및 시간
Time Zone	시간대 선택
Enable NTP	NTP 활성화\비활성화
NTP Server	NTP 서버 IP 주소 설정

표 5- 3 시스템 시간 설정 메뉴

5.4.2 시스템 시간 설정

1. Maintenance> Time Management 메뉴로 접속합니다.
2. 그림 5-12 와 같이 시계 뒤의 동기화 버튼을 클릭한 다음 적용 버튼을 클릭합니다. PC 의 시간이 스위치에 동기화됩니다.
3. 설정 후 Apply 버튼을 클릭합니다.

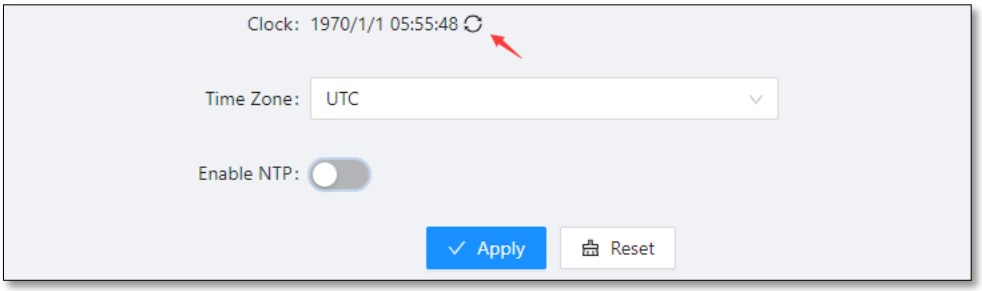


그림 5- 12 시스템 시간 설정

5.4.3 NTP 서버 설정

1. Maintenance> Time Management 메뉴로 접속합니다.
2. Enable NTP 를 활성화합니다.
3. NTP 서버 주소를 입력합니다.
4. 설정 후 Apply 를 클릭합니다.

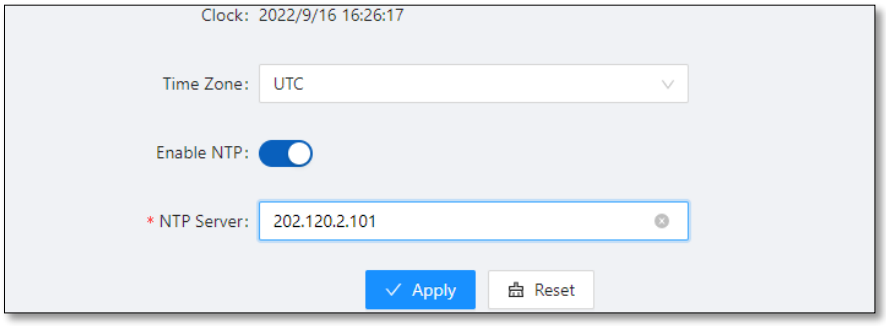


그림 5- 13 NTP 서버 설정

5.5 SNMP

SNMP(Simple Network Management Protocol)는 관리 장치와 네트워크의 관리 장치 간의 통신 규칙을 제공합니다. 이는 관리 장치에서 관리 장치로의 액세스 및 관리를 구현하기 위한 일련의 메시지, 방법 및 구문을 정의합니다. SNMP 에는 다음과 같은 특징이 있습니다.

- 자동 네트워크 관리. SNMP 를 사용하면 네트워크 관리자는 정보를 검색 및 수정하고, 네트워크 문제를 찾아 진단하고, 네트워크 성장을 계획하고, 네트워크 노드에 대한 보고서를 생성할 수 있습니다.
- SNMP 는 다양한 장치 간의 물리적 차이를 보호하므로 다양한 제조업체의 제품을 자동으로 관리할 수 있습니다. 기본 기능 세트만 제공하는 SNMP 는 관리되는 장치의 물리적 기능과 기본 네트워킹 기술 모두로부터 관리 작업을 독립적으로 만듭니다. 따라서 SNMP 는 특히 소규모, 고속, 저비용 네트워크 환경에서 다양한 제조업체의 장치를 효과적으로 관리합니다.

SNMP 메커니즘

SNMP 네트워크는 NMS(Network Management Station)와 에이전트로 구성됩니다.

- NMS 는 SNMP 클라이언트 소프트웨어를 실행하는 스테이션입니다. 사용자 친화적인 인터페이스를 제공하므로 네트워크 관리자가 대부분의 네트워크 관리 작업을 더 쉽게 수행할 수 있습니다.
- 에이전트는 장치에 있는 프로그램입니다. NMS 에서 보낸 요청을 수신하고 처리합니다. 인터페이스 상태 변경과 같은 특정 상황에서만 에이전트가 NMS 에 알립니다. NMS 는 SNMP 지원 네트워크를 관리하는 반면 에이전트는 관리되는 네트워크 장치입니다. NMS 와 에이전트는 SNMP 프로토콜을 통해 관리 정보를 교환합니다.

SNMP 는 다음과 같은 네 가지 기본 작업을 제공합니다.

- Get operation: NMS 는 이 연산을 통해 에이전트의 특정 변수의 값을 획득한다.
- Set operation: NMS 는 이 작업을 통해 에이전트 MIB(Management Information Base)에 있는
- Trap operation: 에이전트는 이 작업을 통해 NMS 에 트랩을 보냅니다.
- Inform operation: NMS 는 이 작업을 통해 다른 NMS 에 트랩을 보냅니다.

• SNMP 설정

1. Maintenance> SNMP 메뉴로 접속합니다.

2. SNMP 버전을 선택하고 사용자, 인증 암호화 비밀번호, 트랩 호스트를 설정한 후 적용 버튼을 클릭하면 설정이 완료됩니다.

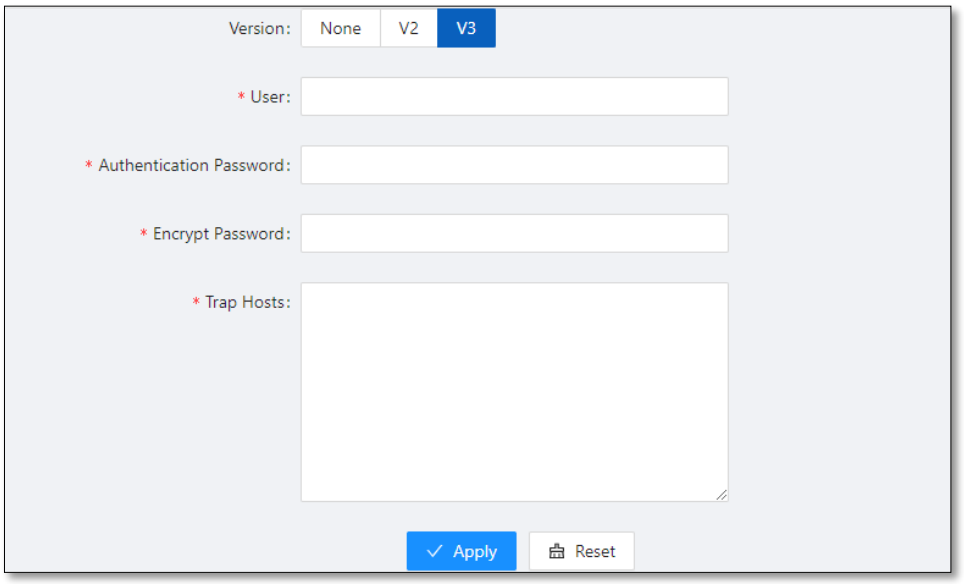


그림 5- 14 SNMP 설정

5.6 Syslog Server

5.6.1 개요

장비 작동 중, 링크 상태 UP, DOWN 등과 같은 다양한 상태 변경이 발생하고, 비정상적인 처리 등과 같은 일부 이벤트도 발생합니다. 시스템 로그는 상태 변경 또는 이벤트 발생 시 고정된 형식으로 메시지를 자동으로 생성하는 일련의 서비스를 제공하며, 이는 장비의 로그 파일에 기록됩니다. 트렁크 포트와 원격 로그인 터미널에 표시될 수 있으며, 관리자가 네트워크 상태를 분석하고 문제를 찾을 수 있도록 네트워크의 1~3 개 로그 서버 그룹으로 전송할 수도 있습니다.

관리자가 로그 메시지를 읽고 관리할 수 있도록 이러한 로그 메시지에 타임스탬프를 지정하고 로그 정보의 우선순위에 따라 등급을 매길 수 있습니다.

5.6.2 syslog 설정

Maintenance > Syslog Server 서버를 선택하여 Syslog 서버 페이지로 접속 합니다.

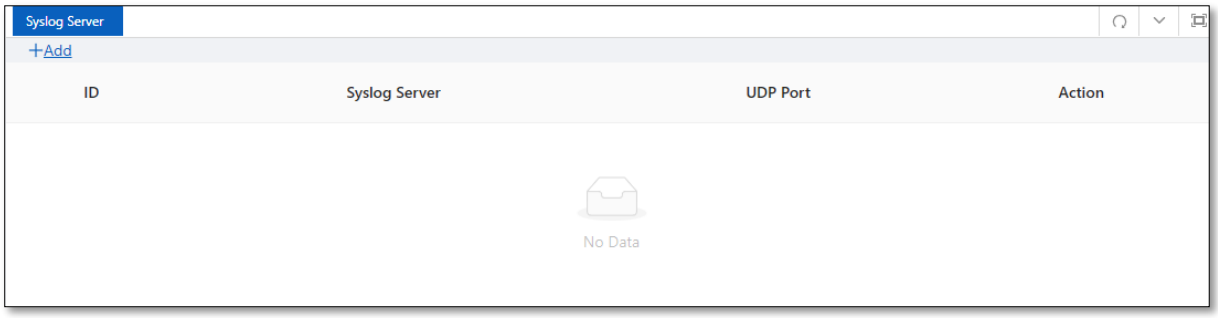


그림 5- 15 syslog 설정

메뉴	설명
ID	Syslog 서버의 ID
Syslog Server	원격 서버의 IP 주소를 구성하고 최대 3 개의 원격 서버 구성을 지원합니다.
UDP port	원격 서버 UDP 프로토콜 포트 구성 지원, 범위 <1-65535>; UDP 포트가 구성되지 않은 경우 기본 포트 번호는 514 입니다.

표 5- 4 syslog 서버설정

1. Maintenance > Syslog Server Syslog 서버 페이지로 들어갑니다.
2. Syslog 서버 아래의 +추가 버튼을 클릭하여 생성 페이지로 들어가 그림 5-16 과 같이 요구 사항에 따라 설정값을 입력하고 확인 버튼을 클릭하여 구성을 완료합니다.



그림 5- 16 syslog 설정

- 설정 예시

장치의 syslog 가 원격 서버로 전송되고 장치의 IP 는 192.168.1.240 이고 원격 서버 IP 는 192.168.1.33 이며 UDP 포트 번호는 10514 입니다.

1. Maintenance > Syslog Server 를 선택하여 Syslog 서버 페이지로 들어갑니다.
2. Syslog Server 아래의 +Add 버튼을 클릭하여 생성 페이지로 이동하고, 요구 사항에 따라 설정 값을 입력하고, OK 를 클릭하여 구성을 완료합니다.
3. Save 를 클릭하여 구성을 저장합니다.



그림 5- 17 syslog 설정 완료

6. Diagnosis

6.1 Network Utilities

6.1.1 개요

- Ping

ping 기능을 사용하여 지정된 주소를 가진 장치에 연결할 수 있는지 확인하고 네트워크 연결을 검사할 수 있습니다. ping 명령을 성공적으로 실행하려면 다음 단계가 필요합니다.

1. 소스 장치는 ICMP 에코 요청(ECHO-REQUEST)을 대상 장치로 보냅니다.
2. 대상 장치는 ICMP 에코 요청을 수신한 후 소스 장치에 ICMP 에코 응답(ECHO-REPLY)을 보내 응답합니다.
3. 소스 장치는 응답을 받은 후 관련 통계를 표시합니다. ping 명령의 출력은 다음과 같습니다.
    - ping 명령은 대상의 호스트 이름이나 IP 주소에 적용될 수 있습니다. 대상의 호스트 이름을 알 수 없는 경우 프롬프트 정보가 표시됩니다.
    - 소스 장치가 타임아웃 시간 내에 ICMP 에코 응답을 받지 못한 경우 Ping 작업 중에 프롬프트 정보와 통계를 표시합니다. 소스 장치가 타임아웃 시간 내에 ICMP 에코 응답을 수신하면 에코 응답 바이트 수, 메시지 시퀀스 번호, TTL(Time to Live), 응답 시간 및 ping 작업 중 통계를 표시합니다. Ping 작업 중 통계에는 전송된 패킷 수, 수신된 에코 응답 메시지 수, 수신되지 않은 메시지 비율, 최소, 평균 및 최대 응답 시간이 포함됩니다.

- Traceroute

Traceroute 명령을 사용하면 소스에서 대상으로 패킷을 전달하는 데 관련된 계층 3 장치를 표시할 수 있습니다. 이 기능은 네트워크 장애가 발생한 경우 장애가 발생한 노드를 식별하는 데 유용합니다.

Traceroute 명령 실행에는 다음 단계가 포함됩니다.

1. 소스 장치는 TTL 값이 1 인 패킷을 대상 장치로 보냅니다.
2. 첫 번째 홉(패킷을 처음 수신하는 계층 3 장치)은 IP 주소가 캡슐화 된 TTL 만료 ICMP 메시지를 소스에 전송하여 응답합니다. 이러한 방식으로 소스 장치는 첫 번째 Layer 3 장치의 주소를 얻을 수 있습니다.
3. 소스 장치는 TTL 값이 2 인 패킷을 대상 장치로 보냅니다.

4. 두 번째 홉은 TTL 만료 ICMP 메시지로 응답하며, 이는 소스 장치에 두 번째 계층 3 장치의 주소를 제공합니다. 이 프로세스는 최종 대상 장치에 도달할 때까지 계속됩니다. 이러한 방식으로 소스 장치는 관련된 모든 계층 3 장치의 주소를 추적하여 대상 장치에 도달할 수 있습니다. Traceroute 명령은 대상의 호스트 이름이나 IP 주소에 적용될 수 있습니다. 대상의 호스트 이름을 알 수 없는 경우 프롬프트 정보가 표시됩니다.

6.1.2 Diagnostic Tool Operation

- Ping Operation

1. Diagnosis> Network Utilities 메뉴에서 IPv4&IPv6 Ping 설정 화면으로 접속합니다.
2. 그림 6-1 과 같이 텍스트 상자에 대상 장치의 IPv4/IPv6 주소를 입력합니다.
3. PING 을 클릭하여 ping 명령을 실행하면 그림 6-2 와 같이 아래 상자에서 결과를 확인할 수 있습니다.

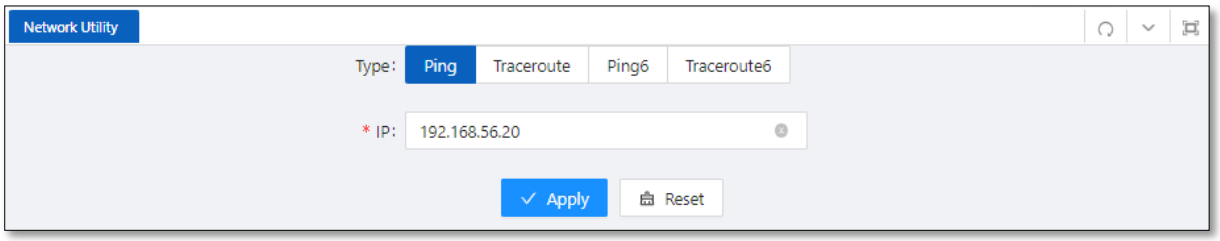


그림 6- 1 Network Utility

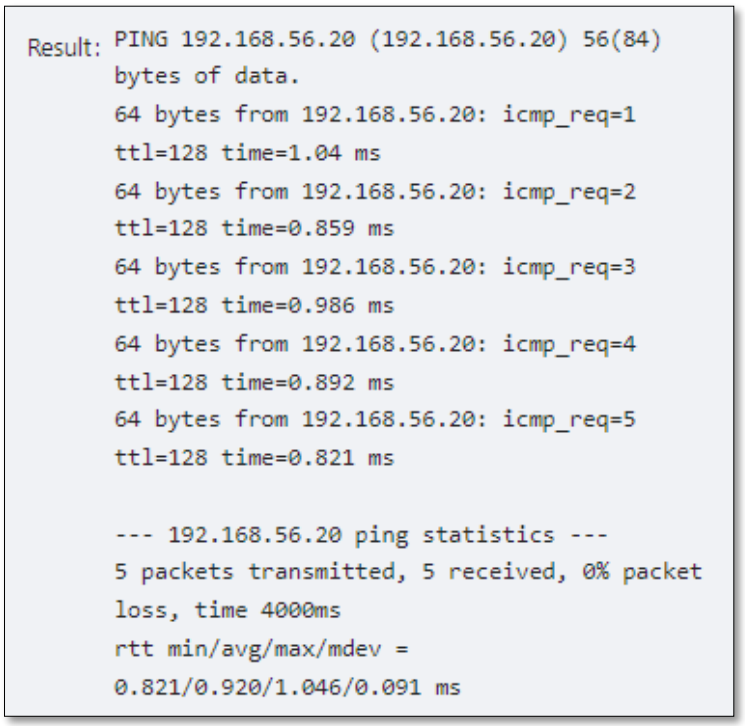


그림 6- 2 핑 테스트 결과

- Traceroute operation

1. Diagnostic> Network Utilities 메뉴로 접속합니다.
2. 텍스트 상자에 대상 IP 주소를 입력합니다.

3. TRACEROUTE 를 클릭하여 경로 추적 명령을 실행하면 그림 6-3 과 같이 아래 상자에 결과가 표시됩니다.

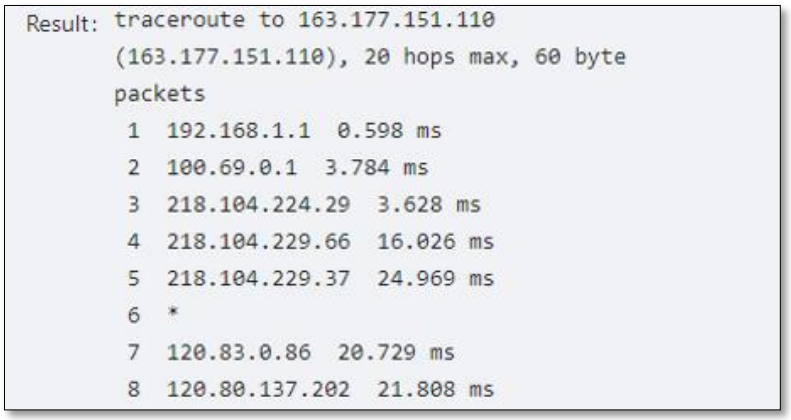


그림 6- 3 Traceroute 결과

6.2 Optical Transceiver Information

장거리 데이터 전송에는 일반적으로 광섬유가 사용됩니다. 그러나 링크에 문제가 발생하면 원격 사이트에서 광섬유 케이블 및 광섬유 트랜시버 문제를 해결하는 데 많은 비용이 듭니다. 이 문제를 해결하기 위해 스위치는 SFP 광섬유 링크에 디지털 진단 및 모니터링(DDM) 기능을 제공하고 사용자가 중앙 사이트에서 광학 매개변수와 성능을 측정할 수 있도록 합니다. 이 기능은 광섬유 링크의 문제 해결 프로세스를 크게 촉진하고 현장 디버깅 비용을 절감할 수 있습니다.

6.2.1 Optical Transceiver Information 보기

1. Diagnosis> Optical Transceiver 메뉴로 접속합니다. 그림 6-4 와 같이 광 모듈의 정보를 자동으로 표시합니다.

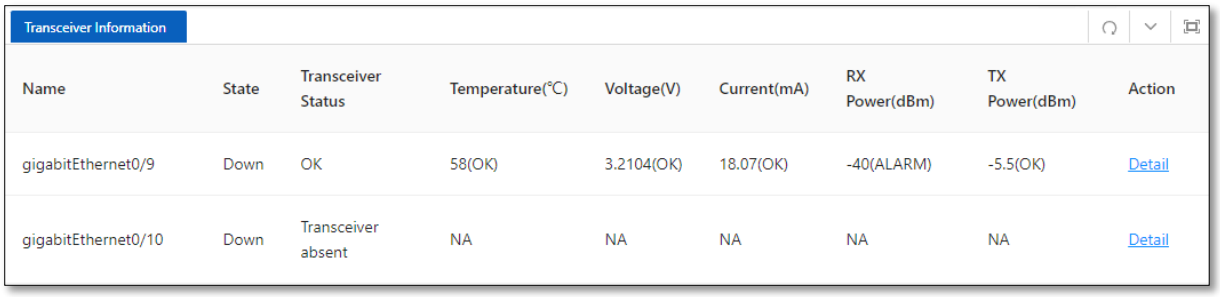


그림 6- 4 광 모듈 정보

메뉴	설명
Name	SFP 가 연결된 스위치 포트 번호입니다.
State	파이버 인터페이스의 상태(동작/동작 중지)입니다.
Transceiver State	트랜시버가 없습니다.
Temperature(degree)	SFP 케이싱 온도
Voltage(V)	트랜시버에 전압 공급.
Current(mA)	트랜시버가 소비하는 전류.
Rx Power(dBm)	광섬유 케이블에서 수신되는 빛의 양
TX Power(dBm)	광섬유 케이블로 전송되는 빛의 양
Detail	클릭하면 세부 정보가 표시됩니다.

표 6- 1 광 모듈 정보 메뉴

6.2.2 Detail Information

1. 인터페이스의 DETAIL 을 클릭하여 트랜시버 세부 정보 페이지로 들어갑니다.

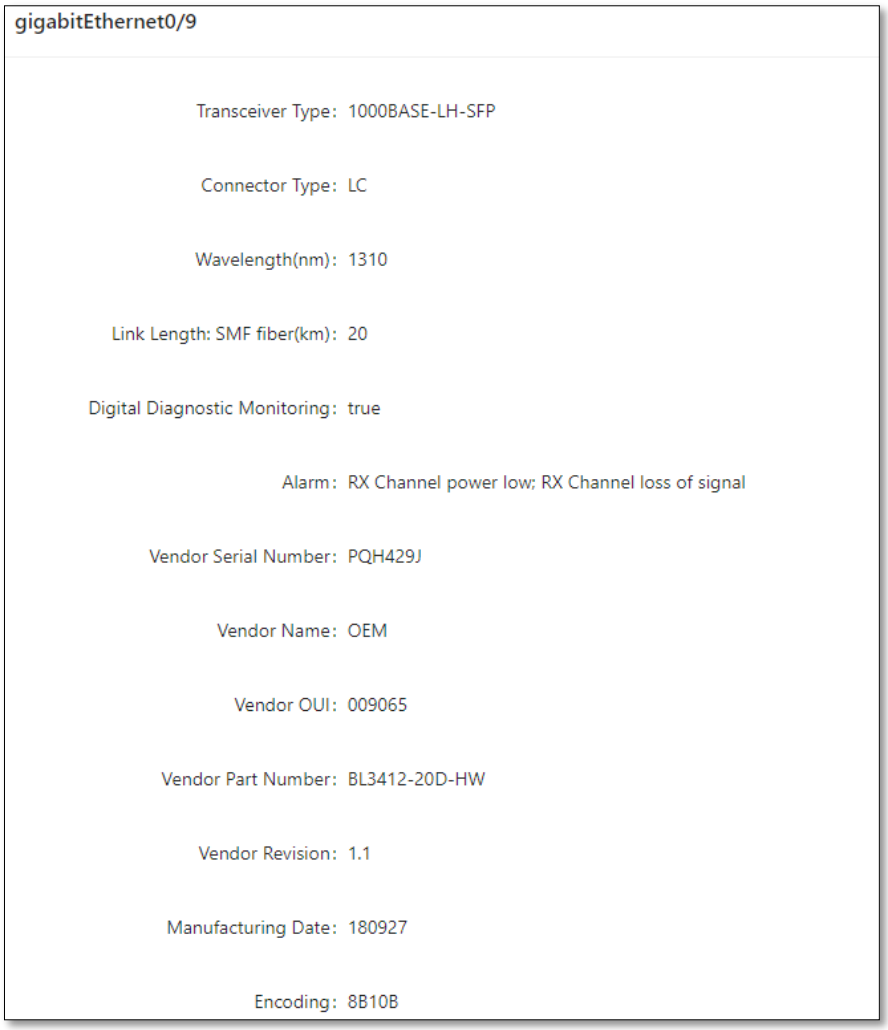


그림 6- 5 세부 정보 메뉴

6.3 One-Click Collection

각 기능에는 고유한 실행 정보가 있으며 일반적으로 각 기능의 출력 정보를 하나씩 확인해야 합니다. 일상적인 유지 관리 중이나 시스템 장애가 발생한 경우 한 번의 작업으로 최대한 많은 정보를 얻기 위해 진단 정보 모듈을 사용하면 여러 기능 정보의 실행 통계를 파일로 저장할 수 있으며, 이 파일을 확인하면 문제를 더 빨리 찾을 수 있습니다.

1. Diagnosis> One-click Collection 메뉴로 접속합니다.
2. click One-click Collection 버튼을 클릭하면 진단 정보 파일이 생성되며, 파일이 생성된 후 파일 다운로드 대화 상자가 나타납니다. 이 파일을 저장할 수 있습니다.

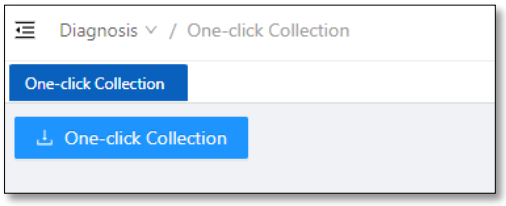


그림 6- 6 One-Click Collection

6.4 Dying Gasp

6.4.1 개요

네트워킹 장치는 커패시터의 임시 백업 전원 공급 장치에 의존하여 정상적인 종료와 Dying Gasp 메시지 생성을 허용합니다. 이 임시 전원 공급 장치는 이러한 작업을 수행하는 데 10~20ms 동안 지속되도록 설계되었습니다. 802.3ah 의 정의에 따르면 장치의 정전 이벤트가 발생하면 장치는 연결된 장치에 OAM 이벤트 메시지를 보냅니다. OAM 은 Point-to-Point 프로토콜이므로 정전 이벤트 메시지는 OAM 을 지원하는 다음 장치로 전송되지 않습니다. 정전 이벤트를 수신한 장치는 정전 로그 프롬프트 메시지를 출력합니다. OAM 경보 정보 외에도 전원 끄기 장치는 SNMP 서버에 트랩 메시지도 보냅니다.

노드 정보	데이터
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

표 6- 2 Dying Gasp

6.4.2 Dying Gasp 설정

1. Diagnosis> Dying gasp 메뉴로 접속합니다.

2. Dying gasp 를 선택하고 적용 버튼을 클릭하여 Dying gasp 를 활성화합니다.

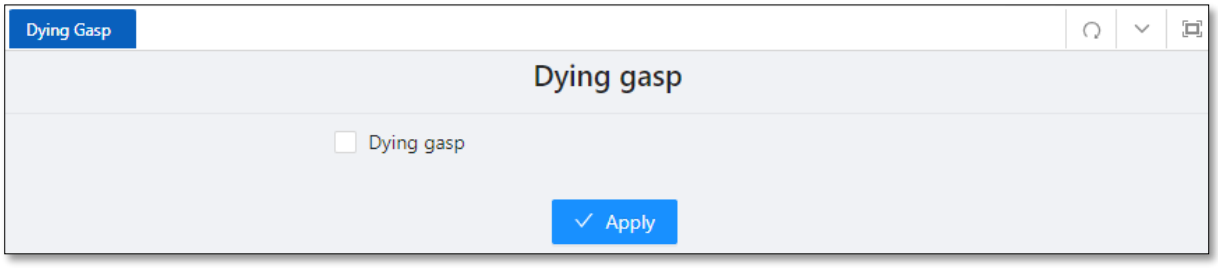


그림 6- 7 Dying Gasp 설정

6.5 Cable Detect

NOTE:

- 이 작업을 수행하면 이미 Up 포트가 자동으로 Down 및 Up 으로 이동하게 됩니다.
- 라인 길이가 6 미터 미만인 경우 테스트 결과와 실제 값 사이에 편차가 있습니다.

케이블 감지는 사용자가 장치의 이더넷 인터페이스에 연결된 케이블의 현재 상태를 감지할 수 있으며 시스템은 5 초 이내에 감지 결과를 확인할 수 있습니다. 감지 내용에는 케이블에 단락 또는 개방 회로가 있는지 여부와 결함이 있는 케이블의 길이가 포함됩니다.

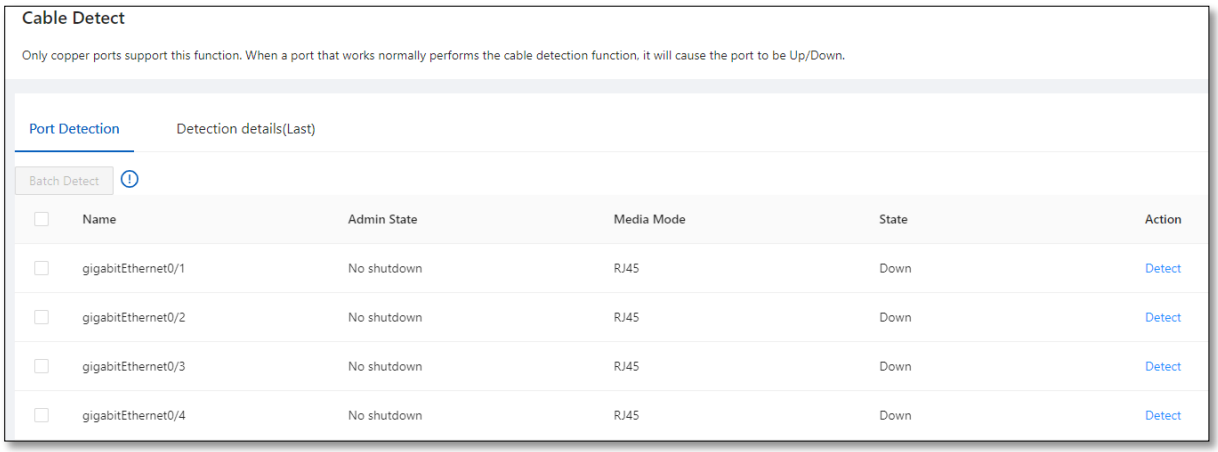


그림 6- 8 Cable Detect



그림 6- 9 감지 결과 화면

NOTE:

- Pair X length: 단위 미터, 케이블 길이, 오류가 발생한 경우 인터페이스에서 오류 위치까지의 길이
- Pair X status

  OK(normal): 라인페어(PAIR)가 정상적으로 종료되었음을 나타냅니다.

  Open: 라인 쌍이 열려 있음을 나타냅니다.

  Short: 쌍의 단락을 나타냅니다.

  Unknown: 기타 알 수 없는 문제